32. JAHRGANG | März 2023 | AUSGABE 3

GIT SICHERHEIT

30 926

MAGAZIN FÜR SAFETY UND SECURITY

Titelthema Seite 20:

ABUS: ZUTRITT PER GESICHT

Innovativ: Interaktionslose Zutrittskontrolle

Mit Heft im Heft ab S. 37

WILEY

Hanwha Techwin

AIoT

AI Kameras passend für die AIoT Revolution

- IoT-fähige Geräte mit MQTT Protokoll
- Cybersicher: UL CAP, NDAA konform, Secure by Default
- Edge-basierte Deep-Learning AI Analytik

www.hanwha-security.eu

Bitte lächeln

Ein freundliches Gesicht kann Türen öffnen. Das ist kein flacher Life-Hack aus dem Readers Digest, sondern gilt ganz buchstäblich – beispielsweise bei den interaktionslosen Zutrittskontrollsystemen mit Gesichtserkennung von Abus Security Center. Wir stellen Ihnen das System in unserer Titelstory ab Seite 20 ausführlich vor – inklusive Interview mit den Geschäftsführern Martin Bemba und Robert Tomic.

Erfreulich finden wir auch die überwältigende Vielfalt an Talk-Gästen und Referierenden, die unsere Einladung zu den nächsten WIN>DAYS im März angenommen haben. Das Motto heißt ja diesmal „Corporate Resilience – Konzepte und Lösungen gegen Angriffe und Gefahren". Die reichhaltige Agenda für die digitale Konferenz – längst eine der wichtigsten Plattformen für den fundierten Austausch für die gesamte Sicherheits-Community – präsentieren wir Ihnen ab Seite 8 dieser Vorfrühlingsausgabe der GIT SICHERHEIT.

Dem Riesenthema Kritis-Sicherheit widmen wir uns in unserem „Heft im Heft" ab Seite 37 – hier nur ein Ausschnitt: Reinhard Rupprecht macht den Einstieg mit einem Übersichtsbeitrag über den Gesamtkomplex der Bedrohung und des Schutzes Kritischer Infrastrukturen – einschließlich eines Mindest-Punkteplans für die Notfallplanung im Unternehmen. Behandelt wird auch das Kritis-Dachgesetz – ein Faden, den Jürgen Seiler des zur Dallmeier-Gruppe gehörenden Consultingunternehmens Davidit in seinem Beitrag „Quo vadis, Kritis" ab Seite 42 aufnimmt. Weiter kommentiert wird dieses aktuelle normative Geschehen anschließend von Johanna Wünsch von Advancis Software & Services: Sie geht der Frage nach, was Betreiber kritischer Infrastrukturen jetzt zur Vorbereitung tun können. Der Rolle privater Sicherheitsdienstleister widmet sich ein Beitrag von Kötter Security (ab Seite 50) – und einen Schwerpunkt auf physische Sicherheit für Kritis ergänzt VfS-Geschäftsführer Prof. Dr. Clemens Gause ab Seite 52. In unserer Brandschutz-Rubrik beschäftigen wir uns unter anderem mit einem Löschkonzept für Züge (ab Seite 66).

Arbeitsschutz ist ein weiterer großer Schwerpunkt dieser März-Ausgabe: Lesen Sie über ein IoT-Leckage-Warnsystem ab Seite 80 und einen dreifach grünen Arbeitsschuh auf Seite 82. Lesen Sie, warum bei Schutzkleidung nicht alles Jacke wie Hose ist (ab Seite 84), dass PSA-Lösungen für alle Arbeitsbereiche Hand und Fuß haben sollten (Seite 86) – oder lernen Sie hammerhartes Schuhwerk mit Tragekomfort kennen (Seite 88) – und alles über Leitersysteme und Steigtechnik (ab Seite 94).

Eine Nachwuchskraft der Sicherheitswelt lächelt Ihnen übrigens auf Seine 14 entgegen: Unter dem Label „Young Security" sprechen wir mit der Bachelor-Studentin Jennifer Dudzik über ihre Erfahrungen mit dem Fach Sicherheitsmanagement an der TH Deggendorf, einem Studiengang zur akademischen Weiterbildung von Sicherheitsfachkräften. Sie arbeitet bereits als Referentin im Ermittlungsdienst am Flughafen München.

Wir wünschen Ihnen gute Erkenntnisse – und dass Sie sicher bleiben.

Ihr

Steffen Ebert
für das Team von Wiley
und GIT SICHERHEIT

QR-Code: Kostenfrei registrieren zur WIN>DAYS-Konferenz „Corporate Resilience – Konzepte und Lösungen gegen Angriffe und Gefahren" (14.–16. März 2023)

TITELTHEMA

Interaktionslose Zutrittskontrolle
Zutrittskontrolle von Abus per Gesichtserkennung

Seite 20

INNENTITEL Safety

Gefahrstofflagerung
Leckage-Warnsystem von Denios

Seite 79

Jennifer Dudzik Thomas Quante Robert Tomic Jürgen Seiler

EDITORIAL

MANAGEMENT

HEFT IM HEFT • KRITIS

Dr. Peter Stahl | Dr. Matthias Rychetsky | Stefan Otto | Christoph Moll

RUBRIKEN

ORGANISATIONEN INSTITUTIONEN UND UNTERNEHMEN IM HEFT INDEX SCHNELLFINDER

NEWS

BDGW: Versuchter Überfall auf ein Geldtransportfahrzeug

Wie die Bundesvereinigung Deutscher Geld- und Wertdienste (BDGW) mitteilt, sollte ein Geldtransportfahrzeug überfallen werden. Am frühen Morgen des 25. Januar 2023 eröffneten unbekannte Täter das Feuer auf ein Geldtransportfahrzeug bei Potsdam an der dortigen Autobahn-Anschlussstelle A 115. Nach Polizeiangaben versuchten die Täter, das Geldtransportfahrzeug zum Anhalten zu zwingen. Dem Fahrer des Geldtransportfahrzeugs gelang es, vor den Angreifern davonzufahren und die Polizei zu alarmieren. Die Täter sind derzeit noch auf der Flucht – die Polizei leitete umgehend eine Fahndung ein. Durch das professionelle Handeln der gut ausgebildeten Sicherheitsmitarbeiter konnte das Anhalten des Fahrzeugs und somit der Raubüberfall auf sie sowie die transportierten Werte verhindert und die Polizei alarmiert werden. Dieser verhinderte Raubüberfall zeigt, dass die Sicherheitsvorschriften der BDGW aus der Anwendung von neuester Sicherheitstechnik für das Spezialgeldtransportfahrzeug und die entsprechende Ausbildung und Schulung von Sicherheitsmitarbeitern durch das betroffene Unternehmen in solchen Sondersituationen durchaus greifen.

www.bdgw.de

© ASW Norddeutschland

Das Gremium der Gründungsmitglieder (v.l.n.r.): Carsten Klauer, Johanna Reidt, Frank Riediger (Handelskammer Hamburg), Klaus Kapinos, Schulleiter Ole Anke, Berit-Kristin Bothe, Peggy Prescher, Jens Müller, Frank Schimmel

ASW Nord: Treffen der Exzellenzinitiative mit Azubis ▲

Ein Treffen der Exzellenzinitiative mit Berufsschülern zeigt eine erfreuliche Entwicklung: Die Sicherheitsbranche wandelt sich. Immer mehr Azubis sind zufrieden mit ihrer Ausbildung zur Fachkraft/Servicekraft für Schutz und Sicherheit.

Die Zahlen sind alarmierend: Trotz wirtschaftlicher Krise fehlt an allen Ecken und Enden Personal – vom hochqualifizierten Meister für Schutz- und Sicherheit, vom Sicherheitsmanager bis hin zur ausgebildeten Fachkraft sowie angelernten Arbeitskraft. Dies hatten schon vor sechs Jahren die Verbände BDSW und ASW Nord, die Handelskammer Hamburg, die Berufliche Schule gewerbliche Logistik und Sicherheit (BS 27) und die Gewerkschaft Verdi erkannt. Man war sich sicher: ein Weg zur Fachkräftesicherung und junge Menschen für die Arbeit in der Sicherheitsbranche zu interessieren ist eine exzellente Ausbildung mit besseren Rahmenbedingungen.

www.aswnord.de

© CES

Ronald Boon (vorne) mit dem internationalen Marketingteam von CES

Ronald Boon ist Marketingleiter bei CES ▲

Ronald Boon ist Leiter des internationalen Marketings bei CES. Er ist seit 2008 in Führungspositionen innerhalb der Unternehmensgruppe tätig, zunächst als Sales Manager und seit 2014 als Geschäftsleiter der niederländischen Tochtergesellschaft CESnederland B.V. in Apeldoorn. Er freue sich auf diese großartige Aufgabe, so Ronald Boon. Zusammen mit seinem internationalen Marketingteam werde man die Markenidentität von CES zeitgemäß gestalten und die Vermarktung der Marke einen Schritt weiterbringen, so Ronald Boon.

www.ces.eu

Christian Cabirol wird CTO bei Mobotix

Chief Technology Officer (CTO) Hartmut Sprave wird die Mobotix AG nach fünfjähriger Tätigkeit auf eigenen Wunsch verlassen. Er möchte sich neuen beruflichen Herausforderungen stellen. Die Nachfolge wird Christian Cabirol antreten. Er wird alle F&E-Schwerpunkte und Technologiepartnerschaften als Schlüsselelemente der lösungsorientierten Strategie verantworten, die auf Qualität „made in Germany“ und höchster Cybersicherheit basieren.

Christian Cabirol ist seit 2016 für Mobotix tätig. Aktuell leitet er die Entwicklung der Kamerasoftware als elementaren Teil der F&E-Strategie. Er wird die Vorstandsposition spätestens zum 1. Juni 2023 von Hartmut Sprave übernehmen.

„Ich begrüße Christian Cabirol herzlich als neuen CTO bei Mobotix“, so der Vorsitzende des Aufsichtsrats, Toshiya Eguchi. Er habe ein hervorragendes Verständnis für die Stärken, die Mobotix sowohl in der Hardware- als auch in der Softwareentwicklung hat, und wie diese weiter ausgebaut werden können. Die strategische Vision von Christan Cabirol für die Entwicklung von nutzenbringenden Lösungen werde dazu beitragen, den Vertrieb weltweit auszubauen.

Mobotix CEO Thomas Lausten bedankte sich herzlich bei Hartmut Sprave für seinen Beitrag und die gute Zusammenarbeit in den vergangenen fünf Jahren. Gleichzeitig gratulierte er Christian Cabirol, der seit seinem Eintritt bei Mobotix seine starken Kompetenzen bereits unter Beweis gestellt habe. Mit seinem Fokus auf Führung und Innovation solle Christian Cabirol die lösungsfokussierte Strategie des Unternehmens weiterentwickeln. Man freue sich darauf, den Kunden und Partnern Christian Cabirols Visionen und Pläne in naher Zukunft zu präsentieren, so Thomas Lausten.

www.mobotix.com

◄◄ zurück zum Inhaltsverzeichnis

Koelnmesse ist Veranstalter der PMRExpo

Die Koelnmesse GmbH ist Veranstalter der PMRExpo. Oliver Freese, COO der Koelnmesse, und Michael Rosenzweig, Geschäftsführer des PMeV – Netzwerk sichere Kommunikation und der PMeV Services GmbH, haben eine entsprechende Kooperationsvereinbarung unterzeichnet. Der PMeV ist Initiator und ideeller Träger der PMRExpo, die erstmals im Jahr 2000 stattfand. 2009 zog sie von Leipzig nach Köln um. Ab der PMRExpo 2023 fungiert die Koelnmesse nun gleichermaßen als Gastgeber und Veranstalter. Gemeinsames Ziel von PMeV und Koelnmesse ist es, das wichtige Themenfeld der sicheren Kommunikation auf alle relevanten Branchen auszuweiten sowie die Internationalisierung der PMRExpo als europäische Leitmesse für sichere Kommunikation weiter voranzutreiben. Hierzu soll auch das Auslandsnetzwerk der Koelnmesse eingebunden werden.

www.pmev.de

Vorstand der Funkwerk AG erweitert

Der Aufsichtsrat der Funkwerk AG hat beschlossen, den Vorstand der Funkwerk AG zu erweitern. Dr. Falk Herrmann ist mit Wirkung zum 1. Februar 2023 zum ordentlichen Mitglied des Vorstands der Gesellschaft bestellt worden. Wesentliche Gründe für diese Entscheidung sind die 2022 stark gewachsene Unternehmensgröße und Führungskomplexität der Funkwerk AG nach der Integration der Hörmann Kommunikation & Netze GmbH (kurz: KN) sowie die angestrebte Umsetzung von Wachstumsstrategien im aufzubauenden neuen Geschäftsfeld Sicherheitstechnik. Darüber hinaus stellt der Aufsichtsrat mit diesem Schritt eine stabile Führung der Funkwerk AG durch den Vorstand sicher und erfüllt so grundlegende Anforderungen eines vorsorglichen Risikomanagements. Dr. Falk Herrmann (52) hat in seiner 20-jährigen Karriere bei der Bosch-Gruppe vor allem im Segment Sicherheitssysteme internationale Managementerfahrung gesammelt.

www.funkwerk.com

© Securitas

Ralf Brümmer (l.) und Arbeitsdirektor Sven Middelhauve

Securitas unterzeichnet Charta der Vielfalt ▲

Securitas hat die Charta der Vielfalt unterzeichnet. Die Charta ist eine Initiative zur Förderung von Vielfalt in Unternehmen und Institutionen unter der Schirmherrschaft von Bundeskanzler Olaf Scholz. Mit der Unterzeichnung setzt das Unternehmen ein klares Zeichen für Vielfalt und Toleranz in der Arbeitswelt und signalisiert die Wertschätzung aller Mitarbeitenden unabhängig von Alter, ethnischer Herkunft und Nationalität, Geschlecht und geschlechtlicher Identität, körperlichen und geistigen Fähigkeiten, Religion und Weltanschauung, sexueller Orientierung und sozialer Herkunft. Unsere Arbeitswelt wandele sich stetig, so Ralf Brümmer, Country President Deutschland. Durch den Einsatz für Vielfalt gelinge die Anpassung an gesellschaftliche und wirtschaftliche Veränderungen wie die Globalisierung, den demografischen Wandel und zukünftig vermutlich sinkende Erwerbstätigenzahlen.

www.securitas.de

©: Klüh/Silke Steinraths

(v.l.n.r.:) Sven Horstmann, Axel Hartmann, Dr. Marc Bieling

Klüh Security erweitert Geschäftsführung zur Dreierspitze ▲

Klüh Security, eine Tochtergesellschaft der Klüh-Gruppe, hat ihre Geschäftsführung neu aufgestellt. Dr. Marc Bieling (48) und Sven Horstmann (47) verstärken die Sicherheitssparte des Multiservice-Anbieters als neue Geschäftsführer neben dem langjährigen Geschäftsführer Axel Hartmann (58). Dr. Marc Bieling leitet die vertriebliche Geschäftsführung, Sven Horstmann und Axel Hartmann verantworten das operative Geschäft. In den zurückliegenden Jahren sei die Security-Sparte des Unternehmens stark gewachsen. Mit Blick in die Zukunft würden jedoch auch die Herausforderungen zunehmen, so Frank Theobald, Sprecher der Klüh-Geschäftsführung. Mit Sven Horstmann und Dr. Marc Bieling habe man zwei sehr erfahrene und profilierte Security-Experten gewonnen, mit denen man die Position am Markt weiter ausbauen werde.

www.klueh.de

QR-Code
zur Anmeldung

PARTNER | SPONSOREN

WIN>DAYS ist eine Serie von Webseminaren – diesmal mit dem Leitmotto „Corporate Resilience – Konzepte und Lösungen gegen Angriffe und Gefahren“.

Corporate Resilience bezeichnet die Widerstandsfähigkeit von Unternehmen, Krisen zu begegnen. Welche Konzepte und Lösungen gibt es, diese Widerstandsfähigkeit weiter zu erhöhen?

Renommierte Experten geben Tipps, Handlungsempfehlungen und Best-Practice-Beispiele. Inklusive Kritische Infrastrukturen, Planung von Sicherheitskonzepten und Corporate Security 4.0.

Tipps, Checklisten, Best Practices für:

- Corporate Safety und Corporate Security Verantwortliche
- Architekten, Planer, Ingenieure und Berater
- Brandschutz-Verantwortliche und Brandschutzbeauftragte
- Errichter, Fachinstallateure und Fachhändler
- Sicherheitsdienste, Polizeien und Behörden
- Sicherheitsbeauftragte
- Facility Manager
- Arbeitssicherheitsmanager
- Sicherheitsingenieure
- Automatisierungstechniker
- Anlagenplaner
- Technische Leiter

Ergänzungen und Aktualisierungen im nächsten Heft sowie laufend auf **www.WileyIndustryDays.com**

AGENDA

AKTUALISIERT

Dienstag März 14

9.45 UHR

9:45 AM - 9:55 AM GMT +1 (10 Min)

Opening Session - Welcome

Dr. Timo Gimbel
Editor & Project Manager
Wiley
Speaker

Lisa Holland
Deputy Editor in Chief
Wiley
Speaker

Dr. Heiko Baumgartner
Publishing Director
Wiley
Speaker

Steffen Ebert
Publishing Director
Wiley
Speaker

Powered By: WILEY

10.00 UHR

10:00 AM - 10:25 AM GMT +1 (25 Min)

Key Note: Corporate Resilience - Konzepte und Lösun Angriffe und Gefahren

Jürgen Wittmann
Director Corporate Security | Präsident
Robert Bosch GmbH | Allianz für Sicherheit in der Wirtschaft BW
Speaker

Powered By:

10.30 UHR

10:30 AM - 11:15 AM GMT +1 (45 Min)

Global Security Governance & Security Risk Managem unternehmerischer Mehrwert oder lästige Policy?

A O
Global Head of Corporate Security (CSO)
DTAG
Speaker

Powered By:

DAIMLER TRUCK

11.30 UHR

11:30 AM - 12:00 PM GMT +1 (30 Min)

Megatrend Sicherheit – Zukunftsstrategien der Corp Security

Julia Vincke
Vice President of Security
BASF
Speaker

Powered By:

BASF
We create chemistry

14.00 UHR

2:00 PM - 2:50 PM GMT +1 (50 Min)

Corporate Security 4.0: Welche sicherheitsbezogenen Herausforderungen sind zu erwarten - und was ist zu

Dr. Jürgen Harrer
Research Coordinator Corporate S...
Technische Hochschule Ingolstadt
Speaker

Benedikt Vetter
Leiter Konzernsicherheit
Würth Group
Speaker

Powered By:

WURTH GROUP

15.00 UHR

3:00 PM - 3:30 PM GMT +1 (30 Min)

Leitstände und Videowände: Sichere Systemlösunger eine Kooperation mit AG Neovo

ÜBERTRAGUNG
Startet 2 Min. vor Beginn des Vortrages

Thore Peters
Senior Sales Manager
AG Neovo Technology BV

Sponsored By:

neovo

15.30 UHR

3:30 PM - 4:15 PM GMT +1 (45 Min)

Videosicherheitskonzepte - wie man Fehler vermeidet, richtig plant und in Betrieb nimmt

Sascha Puppel
CEO, öffentlich bestellter und vereidigter Sachverständiger
Sachverständigen- und Planungsbüro Sascha Puppel GmbH

Powered by:

Mittwoch März 15

10.00 UHR

10:00 AM - 10:40 AM GMT +1 (40 Min)

Krisenvorsorge für Kritische Infrastrukturen - Tipps, Checklisten und Handlungsempfehlungen

Dr. Sandra Kreitner
Notfall- und Krisenmanagerin
Biocelltec GmbH

Powered By:

11.00 UHR

11:00 AM - 11:45 AM GMT +1 (45 Min)

Moderner Brandschutz: Welche Technologien und Lösungen sich für welche Anforderungen besonders eignen - und wie der Brandschutz von morgen aussieht

Michael Hirsch
Vice President Fire Systems
Bosch Building Technologies

Frank Betsch
Prokurist
Securiton

Amela Tinjak
Produktmanagerin Digit...
Hekatron

Matthias Schmölders
Leiter strategische Einh...
Hekatron

BOSCH SECURITON HEKATRON

12.00 UHR

12:00 PM - 1:00 PM GMT +1 (1 Hour)

Lithium-Ionen-Akkus: Kleine Kraftpakete – großes Brandrisiko

Andreas Erbe
Geschäftsführer der Wagner Fire S...
Wagner Fire Safety Consulting Gm...

Felix Prösl
Logistics Solutions
UBH Software & Engineering GmbH

Sponsored By:

WAGNER ubh

14.00 UHR

2:00 PM - 2:30 PM GMT +1 (30 Min)

Cybersicherheit: umfassender, getesteter, zertifizierter Systemschutz für die Zutrittskontrolle

Patrick Bachelart
TIL TECHNOLOGIES GMBH
Speaker

Sponsored By:

TIL TECHNOLOGIES

15.00 UHR

3:00 PM - 3:30 PM GMT +1 (30 Min)

Mobile Credentials: Risiken und Herausforderungen bei Über-Nacht-Lieferungen

Thomas Nieber
Regional Sales Manager DACH
Brivo

Sponsored By:

brivo

16.00 UHR

4:00 PM - 4:45 PM GMT +1 (45 Min)

Künstliche Intelligenz in der Sicherheitstechnik

Prof. Dr. Clemens Gause
Geschäftsführer
Verband für Sicherheitstechnik

Powered By:

VfS

Donnerstag März 16

10.00 UHR

10:00 AM - 10:40 AM GMT +1 (40 Min)

Elf Videoanalysesysteme im harten, aber fairen Vergleichstest: Der GIT System Test Video Analytics. Ein Blick hinter die Kulissen.

Markus Piendl
Geschäftsführer
Sachverständigenbüro Markus Pie...
Speaker

Hannes Dopler
Sachverständiger
Sachverständigenbüro Markus Pie...
Speaker

Powered By:

Sachverständigenbüro
Markus Piendl

10.40 AM

10:40 AM - 11:30 AM GMT +1 (50 Min)

Cyber-Security in der Videoüberwachung - wie lassen sich Systeme sichern?

Katharina Geutebrück
Geschäftsführende Gesellschafterin
Geutebrück GmbH

Sponsored By:

GEUTEBRÜCK

12.00 UHR

12:00 PM - 12:30 PM GMT +1 (30 Min)

Cyberkriminalität im Unternehmenskontext und Lösungsansätze für Errichterbetriebe

Philipp Christopher Rothmann
itsecuritycoach, Inhaber und Director of Coaching
BHE

Powered By:

BHE

14.00 UHR

2:00 PM - 2:30 PM GMT +1 (30 Min)

Die Zukunft der Gefahrstofflagerung

Tobias Authmann
Referent für Sicherheitsschulungen
DENIOS SE

Sponsored By:

DENIOS

15.00 UHR

3:00 PM - 3:45 PM GMT +1 (45 Min)

Der WIN>DAYS Industrie-Talk zum Thema "Industrial Security"

Dr. Gunther Kegel
CEO Pepperl+Fuchs Group / Präsi...
Pepperl+Fuchs Group / ZVEI

Steffen Zimmermann
Leiter des Competence Centers In...
Verband Deutscher Maschinen- u...

Frank Eberle
Advanced Development...
Pilz GmbH & Co. KG

Powered By:

PEPPERL+FUCHS ZVEI: VDMA PILZ MOXA

16.00 UHR

4:00 PM - 4:30 PM GMT +1 (30 Min)

Corporate Security Studie: Warum Unternehmenssicherheit mehr Aufmerksamkeit braucht

Jens Greiner
Director, Forensic Services bei Pw...
PwC PricewaterhouseCoopers

Gunar Korm
Senior Manager, Forensic Services...
PwC PricewaterhouseCoopers

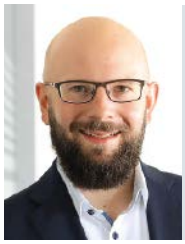
Powered By:

pwc

Stand: 23.02.2023
Ergänzungen und Aktualisierungen im nächsten Heft sowie laufend auf **www.WileyIndustryDays.com**

Hekatron: Bastian Nagel sitzt DKE-Arbeitskreis 713.08 vor

Bastian Nagel, Normen-Experte von Hekatron Brandschutz, sitzt dem neu gebildeten Arbeitskreis der DKE vor. Mit dem Auftrag, die Anwendungsnormen für Gefahrenmeldeanlagen zu vereinheitlichen, hat die Deutsche Kommission Elektrotechnik Elektronik Informationstechnik (DKE) den Arbeitskreis 713.08 gebildet. Die Anwendungsnormen für Gefahrenmeldeanlagen sind in der Normenreihe VDE 0833 verankert. Die entsprechenden Normen werden in Arbeitskreisen des DKE/K713 erarbeitet. Während die DKE das Kompetenzzentrum für elektrotechnische Normung bildet, gilt für Brandmeldeanlagen zusätzlich die DIN 14675-1, die durch das



Bastian Nagel

© Hekatron

Deutsche Institut für Normung aufgesetzt wurde. Bislang unterscheiden sich die miteinander geltenden Anwendungsnormen für Gefahrenmeldeanlagen von ihrem Aufbau her teilweise deutlich. Ziel sei es deshalb, das Normenpaket einheitlicher und damit leichter anwendbar zu gestalten, so Bastian Nagel.

www.hekatron.de

Rohde & Schwarz: Marian Rachow ist Geschäftsführer

Marian Rachow hat die Geschäftsführung der Rohde & Schwarz Cybersecurity GmbH übernommen. In seiner Aufgabe wird er beim IT-Sicherheitsspezialisten den weiteren Wachstumskurs gestalten. Der international erfahrene Manager war zuletzt als CEO von Hensoldt Cyber und Head of Hensoldt Ventures tätig. Der Diplom-Ingenieur hat bei Hensoldt sowie während seiner langjährigen Tätigkeit bei Airbus in den Segmenten Cybersicherheit, Verteidigung, Luft- und Raumfahrt international Managementerfahrung gesammelt. Als Führungskraft in verschiedenen Positionen hat Marian Rachow erfolgreich Strategien für die Entwicklung von innovativen und zukunfts-

Marian Rachow

© Rohde & Schwarz

orientierten Sicherheitslösungen in Wachstumsmärkten umgesetzt. Der bisherige Geschäftsführer Dr. Falk Herrmann hat das Unternehmen auf eigenen Wunsch Ende 2022 verlassen, um sich einer neuen Herausforderung zu widmen.

www.rohde-schwarz.com/cybersecurity

Paxton: Blair Bowen wird Bereichsvorstand

Paxton hat Blair Bowen zum Divisional Director of Manufacturing ernannt, um den Ausbau seiner Fertigungskapazitäten in den kommenden Jahren zu überwachen. Blair Bowen, der vor einem Jahr bei Paxton angefangen hat, habe sich bereits zu einem wichtigen und integralen Mitglied der Geschäftsleitung von Paxton entwickelt, so Adam Stroud, CEO von Paxton. Es sei ein arbeitsreiches Jahr für das Fertigungsteam gewesen, man habe Fortschritte bei der Effizienz erzielt, den Kunststoffspritzguss eingeführt und positive kulturelle Verbesserungen erreicht. Gegenwärtig arbeiten die Fertigungseinrichtungen des Unternehmens nach den

Blair Bowen

© Paxton

Normen ISO 9001 und ISO 14001, die sicherstellen, dass sie sowohl die Qualität als auch Umweltverantwortung betreffend auf höchstem Niveau arbeiten. Unter Blair Bowens Leitung hat das Werk Produktionsrekorde gebrochen und in einem einzigen Monat Produkte im Wert von 7,3 Millionen Pfund hergestellt.

www.paxton-access.com/de/

© Rohde & Schwarz

Rohde & Schwarz vereinbart Kooperation mit TU Chemnitz

Ipoque GmbH – Konzerntochter der Rohde & Schwarz Company – kooperiert mit der Technischen Universität Chemnitz. Das zweijährige Kooperationsprojekt verzahnt Forschung und Entwicklung für eine innovative Softwarelösung, die für Cybersicherheit in 5G-&-6G-Kommunikationsnetzen sorgt. Im Vordergrund steht die Sicherheit bei DDoS-Angriffen (Distributed Denial of Service) und Jamming-Attacken. Da bisher nur wenige praktische Lösungen existieren, eröffnet sich für Ipoque die Chance, unter den ersten Unternehmen mit einer entsprechenden Lösung am Cybersecurity-Markt zu sein. Der Förderaufruf des Bundesamts für Sicherheit und Informationstechnik, dem das Unternehmen im September 2022 folgte, trägt den Titel „Cyber-Sicherheit und digitale Souveränität in den Kommunikationstechnologien 5G/6G“. Fokus des Unternehmens liegt dabei auf der Forschung an einem System, das den Betreibern den sicheren Betrieb von Mobilfunknetzen ermöglicht.

www.rohde-schwarz.com

BHE-Praxis-Ratgeber: Rechtliche Fragen zur Videosicherheit

Der Praxis-Ratgeber des BHE Bundesverband Sicherheitstechnik liefert Antworten auf rechtliche Fragen zur Videosicherheit. Eine übersichtliche Hilfestellung bietet die 5. Auflage des BHE-Praxis-Ratgebers „Videosicherheit“. In dem Buch werden die wichtigsten Rechtsgrundlagen beim Einsatz von Videosicherheitssystemen ausführlich erörtert und umfassend aufbereitet. Im Fokus stehen die Regelungen der geltenden EU-Datenschutzgrundverordnung (DS-GVO) sowie der Neufassung des Bundesdatenschutzgesetzes (BDSG). Der Ratgeber behandelt dabei u. a. die Themenbereiche Interessensabwägung, Speicherung und Löschung, Hinweisbeschilderung sowie Handhabung im Arbeitsumfeld. Er enthält zudem konkrete Beispiele zu unzulässiger Videosicherheit sowie hilfreiche Checklisten für die datenschutzkonforme Planung und Errichtung von Videosicherheitssystemen.

www.bhe.de

◄◄ zurück zum Inhaltsverzeichnis

© Condor

Cornelius Toussaint (l.) von der Condor Gruppe aus Essen und Gerd Kupferer von Securiton bilden das Vorstandsgespann des Fachausschusses Drohnen im BDSW

Securiton im Vorstand des Fachausschusses Drohnen des BDSW

Gerd Kupferer von Securiton ist nun im Vorstand des Fachausschusses Drohnen des Bundesverbands der Sicherheitswirtschaft (BDSW). Drohnen als Einsatzwerkzeug und Risikoparameter gehören für Sicherheitsexperten zum täglichen Geschäft. Ob als Bedrohung für die Sicherheit von Schutzobjekten oder als Einsatzmittel zur Erhöhung und Qualitätssteigerung von Sicherheit, Drohnen sind zwei Seiten einer Medaille. Mit Gerd Kupferer, Bereichsleiter Sicherheits-Speziallösungen aus Achern, und Cornelius Toussaint, geschäftsführender Gesellschafter der Condor Gruppe aus Essen, hat der Fachausschuss Drohnen im BDSW ausgewiesene Experten an Bord. Cornelius Toussaint setzt seit über zehn Jahren auf den Einsatz von Drohnen zu Qualitätssteigerung von Sicherheitsdienstleistungen, und Gerd Kupferer hat langjährige Erfahrung im Bereich der Drohnendetektion und -abwehr.

www.securiton.de

Christophe Leroy ist Business Unit Manager bei Primion

Christophe Leroy ist Business Unit Manager von Primion SAS in Frankreich. Er berichtet direkt an den Managing Director der Azkoyen Time & Security Division, Jorge Pons. Primion SAS ist an zwei Standorten in Frankreich vertreten, dem Hauptsitz in Nanterre und einer Niederlassung im Elsass in Mommenheim. Christophe Leroy hat einen Abschluss in Management/Marketing (Business Administration) an einer amerikanischen Universität und mehr als 20 Jahre Erfahrung auf dem Gebiet der Technologien für den Sicherheitsmarkt. Zuvor hatte er bereits die Position des Geschäftsführers in mittelgroßen und großen internationalen Konzernen inne. Mit seinen ausgeprägten Vertriebs- und Servicekompetenzen bringt er eine neue Dynamik in das französische Team.

www.primion.de

BHE-Fachkongress Brandschutz 2023

Der BHE-Fachkongress „Brandschutz“ öffnet am 19./20. April 2023 zum 9. Mal in Fulda seine Tore. Die Teilnehmer erwartet ein vielseitiges Vortragsprogramm, in dem ausgewählte Referenten aktuelle Entwicklungen und Trends im Bereich Brandschutz präsentieren. Neben modernen Techniken und Brandschutzkonzepten kommen auch die entsprechenden Normen und Regelwerke zur Sprache. Am ersten Veranstaltungstag greift eine Vortragsreihe das Thema „Folgenschwere Fehler bei BMA: Vom Brandschutzkonzept bis zur Sachverständigenabnahme“ auf. Vier Branchen-Experten legen typische Handlungsfehler bei Brandschutzkonzepten, Fachplanungen, Errichtungen und Instandhaltungen von BMA offen und erörtern gemeinsam mit dem Publikum mögliche Lösungsansätze.

www.bhe.de

RISK MANAGEMENT

Sehr oft sind's die eigenen Leute...

Kriminelle Mitarbeiter verursachen mehr Schaden als externe Täter

Schätzungsweise rund 7% der deutschen Unternehmen sind gegen dieses Risiko versichert: Doch wenn Mitarbeiter kriminell werden und das eigene Unternehmen ins Visier nehmen, kann das schnell teuer werden. Deutlich teurer als bei Schäden, die durch externe Täter verursacht werden, also etwa durch Hacker. Zu diesem Ergebnis kommt die jüngste Analyse der Schadensstatistik von Allianz Trade in Deutschland, in der aggregierte Daten aus den Schadensfällen der letzten fünf Jahre in der Vertrauensschadenversicherung (VSV) untersucht wurden.

45 Jahre alt, 10 Jahre im Unternehmen, gebildete Führungskraft: Typisches Täterprofil

Die Schäden durch externe Dritte haben nach der jüngsten Schadensstatistik von Allianz Trade zwar in den vergangenen fünf Jahren mit +40 % bei den Fallzahlen und +56 % bei den Schadenshöhen überdurchschnittlich stark zugelegt: Bei den internen Tätern nahmen Fallzahlen im gleichen Zeitraum um rund 10 % zu und Schäden um 23 %. Dennoch sind es nach wie vor die eigenen Mitarbeiter, die mit 57 % für die meisten und mit rund 70 % auch für die größten Schäden verantwortlich sind.

Die meisten und größten Schäden

„Kriminelle Mitarbeiter sind nach wie vor eine unterschätzte Gefahr in Unternehmen", sagt Rüdiger Kirsch, Betrugsexperte bei Allianz Trade. „Die schwarzen Schafe in den eigenen Reihen richten mit vermeintlichen ‚Alltagsdelikten' wie Betrug, Untreue oder auch Diebstahl und Unterschlagung nach wie vor die größten Schäden an – auch, weil sie mangels Kontrollen oft über viele Jahre unentdeckt bleiben. Vertrauen ist gut, aber es muss seine Grenzen haben. Vor allem ersetzt es keine Kontrollmechanismen: Innentäter sind definitiv kreativ – und Gelegenheit macht Diebe."

Die häufigsten und skurrilsten Motive

Die häufigsten Motive der Täter reichen dabei von Spielsucht, Habgier und luxuriösem Lebensstil bis zu einer finanziellen Notlage, die dann bei den Tätern zu kriminellen Verzweiflungstaten führt. Häufig ist es auch eine Kombination aus verschiedenen Motiven. Mangelnde Wertschätzung oder Rache sind ebenfalls Beweggründe. Einige Fälle in der Schadensstatistik waren allerdings nahezu filmreif und die Gründe ziemlich skurril: Die Innentäter finanzierten mit ihren Machenschaften Schönheitsoperationen, Sportwägen, Luxusimmobilien, Schallplattensammlungen, einen Swingerclub oder ihre krankhafte Tierliebe.

◄◄ zurück zum Inhaltsverzeichnis

Typische Täter kennen Lücken im Kontrollsystem

„Bei den Tätern ist die ganze Bandbreite vertreten. Die größten Schäden verursachen weiterhin männliche Täter im Alter zwischen 40 und Mitte 50, gebildet, in gehobener oder leitender Position im Finanzwesen mit mindestens zehn Jahren Betriebszugehörigkeit", sagt Kirsch. „Sie schlagen zwar seltener zu, aber dann in die Vollen: Sie kennen alle Lücken in den Kontrollsystemen und besitzen durch die langjährige Zugehörigkeit ein entsprechendes Vertrauen von Kollegen und Chefs. Dabei hilft ihnen meist auch ihr freundliches und respektvolles Auftreten – sie sind oft auffällig unauffällig und geraten bei Verdachtsmomenten selten sofort in den Fokus."

Haftungsrisiken häufig unterschätzt

Neben finanziellen Schäden entstehen durch diese Betrugsdelikte auch erhebliche Haftungsrisiken – sowohl für Geschäftsführer als auch für „normale Mitarbeiter". „Wer im Unternehmen entscheidet, haftet", sagt Dr. Stefan Steinkühler, selbständiger Jurist und Experte für Versicherungsrecht, Managerhaftung und Haftungsrecht. „Keine Entscheidung ist in Haftungsfragen aber auch keine Lösung. Kriminelle Mitarbeiter haften für ihre Taten – ihre Chefs aber ebenso, wenn sie es den Tätern zu leicht machen und es unterlassen haben, entsprechende Vorsorgemaßnahmen und Absicherungsmechanismen zu implementieren. Wer seinen Laden nicht im Griff hat, muss dafür geradestehen – schlimmstenfalls mit dem eigenen Privatvermögen. Bestenfalls springt eine Versicherung ein."

Dr. Stefan Steinkühler, Jurist und Experte für Versicherungsrecht, Managerhaftung und Haftungsrecht

Betrogen von Innentätern

Nach Schätzungen von Allianz Trade werden jedes Jahr etwa zehn Prozent der deutschen Unternehmen von ihren eigenen Mitarbeitern betrogen. Die Dunkelziffer ist allerdings hoch. Doch wie können sich Unternehmen vor Innentätern schützen? Vertrauen ist gut – Kontrolle ist besser?

„Die Implementierung von Kontrollmechanismen und Compliance-Systemen sowie Routine-Kontrollen und Audits sind für Unternehmen tatsächlich ein entscheidender Baustein, um sich zu schützen", sagt Steinkühler. „Aber auch die Sensibilisierung und Schulung der Mitarbeiter für interne Richtlinien, kritische Situationen und die Detektion von Auffälligkeiten sind Faktoren, die wesentlich zum Schutz vor Innentätern beitragen. Mit diesen Maßnahmen schaffen sie gleich doppelten Schutz: für das Unternehmen einerseits und für die Minimierung der eigenen Haftungsrisiken andererseits."

Vertrauen und Kontrolle müssen sich die Waage halten

Kontrolle ist aber längst nicht alles und ein Übermaß der Kontrolle kann bei mangelndem Vertrauen auch schnell nach hinten losgehen. „Für die Unternehmen ist es deshalb wichtig, dass sie eine Balance zwischen Vertrauen und Unternehmenskultur auf der einen Seite und Vorsorge und Kontrolle auf der anderen Seite finden", sagt Kirsch. „Zufriedene Mitarbeiter, denen Kollegen und Vorgesetzte mit Respekt und Wertschätzung begegnen und die mit Aufgaben und Bezahlung sowie Aufstiegsmöglichkeiten zufrieden sind, identifizieren sich mit dem Unternehmen und sind in der Regel wesentlich loyaler als Mitarbeiter, die kein gutes Betriebsklima vorfinden."

Mobbing, Frustration und Rache sind häufige Motive, die interne Täter antreiben. Die Unternehmens- und Fehlerkultur sowie die offene und transparente Kommunikation spielen also eine entscheidende Rolle. Wenn Mitarbeitende sich trauen, Missstände anzusprechen, können Schwachstellen identifiziert, Sicherheitslücken geschlossen und Täter schneller identifiziert werden. „Whistleblowing" spielt deshalb neben den internen Kontrollmechanismen bei der Prävention die Hauptrolle. Die meisten Betrugsfälle in Unternehmen werden bei der Revision, bei sonstigen Routineprüfungen oder bei der Überprüfung von Auffälligkeiten aufgedeckt. Aber auch Hinweise von anderen Mitarbeitenden führen oft zur Überführung der internen Täter.

Anonymisierte Kanäle schützen Hinweisgeber

Gerade deswegen gewinnt der Entwurf für das Hinweisgeberschutzgesetz (HinSchG), das Ende 2022 in Kraft treten soll, immer mehr Bedeutung: Unternehmen müssen entsprechende interne Kanäle einrichten, die jene schützen, die Auffälligkeiten melden. Zufallsfunde gibt es ebenfalls – und in ganz seltenen Fällen plagt die Betrüger im Nachgang ein schlechtes Gewissen, so dass sie sich selbst anzeigen.

„Selbstanzeige ist allerdings noch selten", sagt Kirsch. „Unternehmen sollten daher lieber auf eine gute Unternehmenskultur, Compliance und den Schutz von Hinweisgebern setzen. Denn die meisten Innentäter haben ein hohes Maß an krimineller Energie und ihr moralischer Kompass ist meist außer Betrieb. Sie nutzen Gelegenheiten umgehend. Deshalb sollten sich Unternehmen nicht in falscher Sicherheit wiegen und permanent mögliche Sicherheitslücken überprüfen und schließen."

Rüdiger Kirsch, Betrugsexperte bei Allianz Trade

„Nur anonymisierte Hinweisgebersysteme schützen wiederum den Hinweisgeber vor Repressalien", sagt Steinkühler. „Die Einführung eines Whistleblowing-Systems zur frühzeitigen Identifizierung von Risiken kann Unternehmen und Geschäftsleiter vor Haftung und Geldbußen schützen." ●

Eine Umfangreiche Analyse mit Statistiken, zahlreichen Beispielfällen, Täterprofilen, (skurrilen/häufigsten) Motiven, Haftungsfallen sowie damit verbundenen Themen wie Whistleblowing / Hinweisgeberschutzgesetz und wie Unternehmen sich schützen können inkl. Checklisten findet sich auf GIT-SICHERHEIT.de - unter dem Beitrag PDF-Download: https://bit.ly/3sebunb

Allianz Trade Deutschland
Hamburg
www.allianz-trade.de

◄◄ zurück zum Inhaltsverzeichnis

YOUNG SECURITY

Turbo für die Karriere in der Sicherheit

Bachelor-Studium Sicherheitsmanagement an der TH Deggendorf

Jennifer Dudzik ist Referentin Ermittlungsdienst am Flughafen München – und eine der Studentinnen des Bachelor-Studiums Sicherheitsmanagement an der TH Deggendorf

Die Technische Hochschule Deggendorf bietet seit 2019 den berufsbegleitenden Studiengang Sicherheitsmanagement an. Diese einzigartige Möglichkeit zur akademischen Weiterbildung von Sicherheitsfachkräften wurde vom BVSW initiiert, gemeinsam mit Sicherheitsexperten aus der Industrie sowie der öffentlichen Hand. Auch die Polizei in Niederbayern ist Kooperationspartner. Mittlerweile stehen die ersten Studierenden kurz vor ihrem Abschluss. Jennifer Dudzik, Referentin Ermittlungsdienst am Flughafen München, ist eine von ihnen und berichtet im Interview über ihre Erfahrungen.

GIT SICHERHEIT: Frau Dudzik, seit wann arbeiten Sie im Sicherheitsbereich? Was ist ihre derzeitige berufliche Tätigkeit?
Jennifer Dudzik: Im September 2016 habe ich mit der Ausbildung zur Fachkraft für Schutz und Sicherheit am Flughafen München begonnen. Da ich meine Ausbildung verkürzen konnte, habe ich diese bereits nach 2,5 Jahren abgeschlossen und wurde als Assistentin des Leiters Konzernsicherheit übernommen. Mittlerweile bin ich als Referentin Ermittlungsdienst am Flughafen München tätig. In dieser Position bin ich unter anderem die Ansprechpartnerin für Polizei und Behörden und übernehme die interne Koordination bei Ermittlungen.

Mit welcher Motivation haben Sie das Studium Sicherheitsmanagement an der TH Deggendorf aufgenommen?
Jennifer Dudzik: Während meiner Ausbildung konnte ich das umfangreiche Aufgabenspektrum in der Sicherheit kennenlernen, u. a. mit Stationen bei der Einsatzleitstelle der Konzernsicherheit, in der Abteilung für Sicherheitsrichtlinien und -konzepte, bei den Hundeführern und auch bei der Flughafenfeuerwehr. Das hat mir gezeigt, wie unglaublich spannend und vielseitig dieser Bereich ist. Zum anderen gibt es momentan noch verhältnismäßig wenig Mitarbeiter in der Sicherheit mit Abschluss in einem Sicherheitsmanagementstudium, obwohl durchaus Bedarf besteht, der mit der zunehmenden Komplexität der Aufgaben ständig wächst. Da habe ich in dem Studium die Chance gesehen, mir weitere berufliche Möglichkeiten zu erschließen.

Können Sie kurz beschreiben, wie das Studium abläuft?
Jennifer Dudzik: Das Studium umfasst insgesamt elf Semester, wobei zwei Semester davon Praxissemester sind. Weil ich bereits im Sicherheitsbereich tätig bin, konnte ich mir meine berufliche Erfahrung anrechnen lassen. Damit bin ich derzeit im neunten Semester und stehe kurz vor dem Abschluss.

◄◄ zurück zum Inhaltsverzeichnis

Sicherheitsmanagement-Studenten begleiten Polizei beim Eishockeyspiel der Straubing Tigers: Kriminalrat Christoph Gibis mit Studenten der THD

Am Ende eines jeden Semesters werden Prüfungen abgenommen, abhängig vom Fach entweder mit einer Studienarbeit oder einer schriftlichen Klausur.

Wie lassen sich Vollzeitjob und Studium miteinander vereinbaren?

Jennifer Dudzik: Die Vorlesungen finden ausschließlich Freitag nachmittags und Samstag ganztägig statt. Beim Flughafen München kann ich in meiner Position in Gleitzeit arbeiten, was für ein berufsbegleitendes Studium ein enormer Vorteil ist. Damit kann ich meine Arbeitszeit so einteilen, dass ich Freitagnachmittag zur Hochschule nach Deggendorf aufbrechen kann. Außerdem bietet die Hochschule mittlerweile einige Vorlesungen in hybrider Form an, das heißt es besteht die Möglichkeit, in Präsenz oder online daran teilzunehmen. Damit gestaltet sich das Studium nochmal ein ganzes Stück flexibler.

Bieten Ihnen die Fächer und Themen im Studium bereits Anknüpfungspunkte für Ihre aktuelle berufliche Tätigkeit?

Jennifer Dudzik: Durchaus. Unsere Dozenten kommen oft aus der Praxis, zum Teil selbst aus der Konzernsicherheit, und haben einen großen Erfahrungsschatz, von dem alle Studierenden profitieren. Wir können uns jederzeit mit Fragen an sie richten, auch noch nach Abschluss des jeweiligen Studienmoduls.

Was gefällt Ihnen besonders an dem Studium?

Jennifer Dudzik: Besonders gefällt mir die Verknüpfung von Sicherheits- und Managementthemen. Die wirtschaftlichen Aspekte der Sicherheit werden besonders bei Führungspositionen in dem Bereich immer wichtiger. Außerdem geben die Fächer den Studenten die Möglichkeit, auch in anderen Bereichen zu arbeiten, in denen unternehmerisches Denken gefordert wird.

Wie ist der Kontakt zu Ihren Kommilitonen bei dem berufsbelgleitenden Studiengang?

Jennifer Dudzik: Meine Kommilitonen, sowie die aus den nachfolgenden Semestern, kommen aus ganz unterschiedlichen Sicherheitsbereichen, etwa von einem Sicherheitsdienstleister, der Bundeswehr oder auch der Polizei. Somit bringt jeder unterschiedliche Kompetenzen mit, so dass wir auch viel voneinander lernen können. Mittlerweile sind wir ein gutes Team geworden und haben auch über die Vorlesungen hinaus immer wieder Kontakt.

Wenn Sie Ihren Bachelor in der Tasche haben, was ist Ihr nächstes berufliches Ziel?

Jennifer Dudzik: Da ich erst seit ein paar Monaten meine aktuelle Position innehabe, hat für mich zunächst das Sammeln von Berufserfahrung Priorität. Da man sich bei uns innerhalb der Konzernsicherheit aber gut weiterentwickeln kann, bin ich gespannt und offen dafür, was sich für mich in den nächsten Jahren bereithält. ●

Infos zum Bachelor-Studium Sicherheitsmanagement an der TH Deggendorf finden Sie hier: https://www.th-deg.de/de/weiterbildung/bachelor/sicherheitsmanagement

Campus der Technischen Hochschule Deggendorf

© Bilder: TH Deggendorf

Bayerischer Verband für Sicherheit in der Wirtschaft e. V.
München
Tel.: +49 89 357 483 0
info@bvsw.de
www.bvsw.de

◄◄ zurück zum Inhaltsverzeichnis

ENERGIE & NACHHALTIGKEIT

Für ein besseres Leben

Thomas Quante über sichere Wege zur Energieeffizienz, CO_2-Neutralität – und über Bosch als Wunsch-Arbeitgeber

GIT SICHERHEIT sprach mit Thomas Quante, CEO von Bosch Building Technologies. Das Gespräch fand auf der „Bosch Connected World" in Berlin statt, einem internationalen Branchenevent für Digitalisierung und Künstliche Intelligenz. Im Interview verrät er, wie der Gebäudesektor global zu mehr Energieeffizienz, Nachhaltigkeit und Sicherheit beitragen kann, welche branchenweiten Allianzen sich jetzt formieren und was es braucht, um ein attraktiver Arbeitgeber zu sein.

GIT SICHERHEIT: Herr Quante, auf der Bosch Connected World geht es um die Verbindung von Künstlicher Intelligenz und dem Internet der Dinge, also AIoT, um digitale Transformation. Wenn wir den Rahmen ganz groß spannen: Die BCW findet vor dem Hintergrund des Klimawandels, der Energieknappheit und des Ringens um Nachhaltigkeit statt. Wie positioniert Bosch Building Technologies sich hier?

Thomas Quante: Energieeffizienz, Nachhaltigkeit und Komfort sind für uns als Lösungsanbieter für kommerzielle Gebäude und Industrieanwendungen zentrale Themen. Menschen sollen sich in Gebäuden und kritischer Infrastruktur sicher und wohl fühlen. Gebäude können einen großen Beitrag zur Reduktion von Treibhausgasen leisten – die unserer Kunden und auch unsere eigenen. Das alles auch angesichts zunehmender Berichtspflichten für Unternehmen in puncto ESG-Reporting…

… sprich das Unternehmens-Reporting über Environment, Social und Governance, also die Offenlegung von Umwelt-, Sozial- und Corporate-Governance-Berichtspflichten.

Thomas Quante: Richtig. In Sachen E-Mobilität haben wir uns als Gesellschaft bereits auf einen sehr guten Weg gemacht, klimafreundlicher unterwegs zu sein. Jetzt richtet sich der Blick verstärkt auf den umweltfreundlichen Betrieb von Gebäuden und Anlagen. Auch hier ist die Energiebilanz sehr wichtig, um den CO_2-Footprint zu verringern. Immerhin stammen 40 Prozent der weltweiten CO_2-Emissionen aus dem Gebäudesektor.

Wie sieht das konkret aus?

Thomas Quante: Ein Beispiel: Menschen sollen sich auch an ihren Arbeitsstätten wohlfühlen. Gleichzeitig hält das hybride Arbeiten allerorts Einzug. Es gilt also, Gebäude und Arbeitsräume so zu gestalten, dass sie energieeffizient und nachhaltig sind, wenn Mitarbeitende zum Beispiel nur noch zwei oder drei Tage pro Woche ins Büro kommen. Idealerweise werden deren Arbeitsräume nicht mehr durchgängig geheizt, sondern nur noch dann, wenn es notwendig ist.

All diese Überlegungen haben übrigens auch dafür gesorgt, dass wir mit unserem Bosch-Geschäftsbereich Building Technologies an einen neuen Standort ziehen werden. Dahinter steht ein ganz neues Konzept, das hybrides Arbeiten vereinfacht und uns so gerade auch für neue Mitarbeitende noch attraktiver als Arbeitgeber macht. Die Fläche in unserer zukünftigen Niederlassung – die CO_2-neutral ist – beträgt dann nur noch 60% der bisher beanspruchten Fläche. Statt fester Büros bieten wir künftig auch Co-Working-Spaces für diejenigen an, die nur noch selten im Büro sind.

Was ist generell das große Ziel, die Mission hinter dem Engagement von Bosch Building Technologies für mehr Nachhaltigkeit?

Thomas Quante: Wir wollen bei unseren Kunden, genau wie auch bei uns selbst, den Energiebedarf und die daraus resultieren-

◀◀ zurück zum Inhaltsverzeichnis

den Emissionen minimieren, dadurch Kosten einsparen und die Umwelt schonen. Das alles ganz nach unserer Mission „Gebäudelösungen für ein besseres Leben“. Damit begegnen wir dem steigenden Bedarf an Sicherheit, Komfort und Energieeffizienz.

Welche konkreten Beispiele können Sie nennen?

Thomas Quante: Einen wichtigen Beitrag zur Klimaneutralstellung leistet die „Energy Platform“ von Bosch Building Technologies – unsere umfassende, cloudbasierte Anwendung mit Echtzeitanalyse von Energiedaten. Sie ist schon in über 120 Bosch-Werken und -Standorten weltweit im Einsatz und optimiert den Energieverbrauch der gesamten Bosch-Gruppe. Wichtig für unsere Unternehmensstrategie sind auch die Übernahmen von erfahrenen Gebäudeautomations-Unternehmen: Climatec aus den USA sowie die GFR und Hörburger in Deutschland. Diese gehören seit 2015, 2019 bzw. 2021 zur Bosch-Familie. Mit diesem starken Team, deren Kernkompetenzen und Lösungen, sind wir auf dem besten Weg, den Betrieb von Gebäuden weiter zu optimieren.
Mit der Gründung der Bosch Climate Solutions GmbH als Beratungsunternehmen helfen wir zudem anderen Unternehmen mit unserem Know-how auf dem Weg zur CO_2-Neutralität. Bosch Climate Solutions ist inzwischen Teil von Bosch Building Technologies. Es gibt schon rund 30 Referenzkunden, darunter namhafte Unternehmen wie Trumpf, Würth, Kistler und Chiron.

In Summe bietet Bosch Building Technologies ein umfassendes Leistungsportfolio: von der Beratung bis hin zur konkreten Umsetzung durch unser Systemintegrator-Geschäft und der Betreuung über den gesamten Lebenszyklus.

Auf der Light + Building 2022 gab es erste Einblicke in die digitale Service Suite „Nexospace“. Was ist der Kern dieses Angebots, welche konkreten Services sind das?

Thomas Quante: Mit der cloudbasierten Plattform Nexospace betreiben wir eine Daten-Autobahn – und diese Autobahn stellen wir mittlerweile auch Dritten zur Verfügung. Es geht um die zielgerichtete Auswertung von Sensordaten für ein komfortables und ganzheitliches, digitales Management kommerzieller Gebäude. Unter dem Namen Nexospace werden erstmals sämtliche IoT-gestützte Servicelösungen für Gebäudemanagement gebündelt. Die aggregierte Datenanalyse aus allen Systemen der Gebäudetechnik zeigt dabei Verbesserungspotenziale auf und sorgt darüber hinaus für reibungslosere Betriebsabläufe.

Wir sind hier bereits mit drei Services gestartet: Der „Nexospace Fire Sys-

Thomas Quante (l.), CEO von Bosch Building Technologies, und GIT-Chefredakteur Steffen Ebert auf der Bosch Connected World 2022 in Berlin

◄◄ zurück zum Inhaltsverzeichnis

Bosch Connected World 2022

Die Bosch Connected World hat es sich seit 2014 zur Aufgabe gemacht, AIoT und digitale Transformation in den Vordergrund zu rücken. Mit ihrer Konferenz, der Ausstellung und den zahlreichen Vernetzungsmöglichkeiten entwickelt sich die jährliche Veranstaltung stetig weiter, so auch am 9. und 10. November 2022 in Berlin. Auch online konnte an dem Event teilgenommen werden.

Konferenzeröffnung – hier mit Bosch-Geschäftsführer Stefan Hartung (l.) und Moderator Dirk Slama. Im Bildschirm: KI-Pionier Andrew Ng

Hauptredner: Bosch-Chef Stefan Hartung

Vortragende: Thomas Quante (Bosch Building Technologies), Moderatorin Jennifer Sarah Boone, Marcus Nadenau (Bosch Building Technologies), Dirk Dittrich (Edge), Andreas Kühne (Bauakademie), Dominik Brunner (Arelio), Jan von Mallinckrodt (Union Investment RE), Johannes Kreissig (DGNB) und Andreas Mauer (Bosch Building Technologies)

Konferenzteil

Die Besucher hatten die Möglichkeit, auf vier Bühnen Keynotes, fachbezogene Breakout-Sessions, Podiumsdiskussionen, Expertengespräche und -interviews sowie Workshops zu verfolgen. Das Programm konzentrierte sich auf die nächste Welle der digitalen Transformation und den Wandel zu digitalen OEMs. In einer Vielzahl von Sitzungen wurden Strategien, Best Practices und Fallstudien zu intelligenten, vernetzten und nachhaltigen Produkten und Lösungen vorgestellt, die durch AIoT ermöglicht werden. Nachhaltiges Handeln durch Energie- und Ressourceneinsparung war zentraler Aspekt in allen Sessions.

Hybride Ausstellung

In der Hybrid-Ausstellung präsentierten sich Bosch und mehr als 80 KI- und IoT-Unternehmen sowie innovative Start-ups auf 6.000 Quadratmetern Ausstellungsfläche in Berlin und „unzähligen" Quadratmetern online. Das neudeutsch genannte „Ökosystem", bestehend aus Bosch, seinen Kunden und Partnern, traf sich, um Produkte, Software und Dienstleistungen im Bereich AIoT zu präsentieren. Dazu gehörten Bereiche wie Gebäude, Energie, Logistik, Fertigung, Mobilität, Smart Life und Transport.

Keynote: CEOs von Bosch und BMW

In der Eröffnungs-Keynote sprachen Stefan Hartung, Vorsitzender der Bosch-Geschäftsführung, und Oliver Zipse, Vorsitzender der BMW-Geschäftsführung, über die Zukunft der Mobilität – wie Digitalisierung, Elektrifizierung und Nachhaltigkeit die Branche verändern. Oder auch, was die etablierten Unternehmen von Mobilitäts-Start-ups lernen können und umgekehrt. Andrew Ng, Gründer & CEO von Landing AI und einer der bekanntesten KI-Experten weltweit, gab einen Einblick, wie Künstliche Intelligenz als disruptive Technologie den digitalen Wandel nicht nur in der Mobilität vorantreibt.

Nachhaltiger Lebenszyklus von Gebäuden

Verbesserungen im Gebäudebetrieb können enorme Auswirkungen auf die Zufriedenheit der Mieter, Nachhaltigkeit, Effizienz und Sicherheit haben. Zu den Hauptthemen der Sondersitzung „Nachhaltiger Gebäudelebenszyklus", die von Thomas Quante, CEO von Bosch Building Technologies, geleitet wurde, gehörten Gebäudeautomation, Sicherheit und Energieeffizienz. Das Auditorium erhielt Hinweise, wie modernste AIoT-Technologie helfen kann, Energieeffizienzziele zu erreichen. In Podiumsdiskussionen und Vorträgen wurde diskutiert und dargestellt, inwieweit die Themen Energieeffizienz und Nachhaltigkeit bereits in der Immobilienbranche angekommen sind – mit der Antwort, dass man hier noch ganz am Anfang stehe. Und dass das Thema ESG noch nicht klar genug interpretiert werde. Nach einigen Antworten und Praxisbeispielen schloss diese Session die Building-Lifecycle-Diskussion mit einer ganzheitlichen Perspektive auf den Gebäudebetrieb ab – und mit einer Präsentation des neuen Bosch-Angebots Nexospace durch Chief Architect Andreas Mauer.

tem Analyzer" ermöglicht einen schnellen Überblick zum Zustand der Brandmeldeanlagen von jedem Ort aus. Ein Cockpit zeigt den aktuellen Systemstatus, das digitale Betriebsbuch und den Plan für künftige Austauschaktivitäten an und erleichtert so die Investitionsplanung. Für die effiziente Gebäudeautomation gibt es den „Nexospace Performance Optimizer" zur stetigen Analyse von Leistungs- und Verbrauchsdaten aus der Gebäudetechnik, der sich noch in der Pilotphase befindet. Der „Nexospace Cyber Security Guard" dient als Schutz für windowsbasierte Sicherheitssysteme vor Viren und anderer Malware, also als Service zur Vermeidung möglicher Cyberangriffe.

Bedeutet das künftig: „iPad statt Schraubendreher"?

Thomas Quante: (lacht) Das könnte man denken. Tatsächlich sind wir mitten in der digitalen Transformation und es gilt auch, die gesamte Mannschaft auf diese Reise mitzunehmen. Deswegen ist die Kombination wichtig: erfahrene Service-Technikerinnen und -Techniker, die zum Beispiel eine komplizierte Instandsetzung vornehmen können, und ausgewiesene digitale Spezialistinnen und Spezialisten.

Bei allem Bemühen um Nachhaltigkeit für Ihre Kunden: Wie steht es aktuell um den eigenen ökologischen Fußabdruck von Bosch?

Thomas Quante: Natürlich gilt es bei allen Initiativen, zunächst auch im eigenen Haus anzufangen. Bei Bosch arbeiten wir intensiv an Maßnahmen zur Erreichung der Klimaneutralität. Und das mit vier Hebeln: Erstens eine deutliche Steigerung der Energieeffizienz – dafür steht bis 2030 ein jährliches Budget von 100 Millionen Euro zur Verfügung. Der zweite Hebel ist „New Clean Power", womit Bosch die regenerative Energieerzeugung aus eigener Produktion ausweiten und bis 2030 400 Gigawattstunden jährlich selbst produzieren will. Drittens der Einkauf von grünem Strom. Und der vierte Hebel: Kompensationsmaßnahmen nur für unvermeidbare Emissionen.

Zurück zu Ihrem Angebot für den Gebäudesektor. Arbeiten Sie auch mit anderen Partnern zusammen, um diese komplexen Herausforderungen zu meistern?

Thomas Quante: Das geht definitiv nicht alleine. Wir sind fest davon überzeugt, dass es eine enge Zusammenarbeit auch mit anderen Anbietern braucht. Mit aktuell 45 Partnern entwickeln wir gerade ein offenes, domänenübergreifendes und cloudbasiertes Ökosystem. Dabei geht es um die Kombination und Integration aller Gebäudesysteme,

◄◄ zurück zum Inhaltsverzeichnis

Dienste und Softwarelösungen aus verschiedensten Anwendungsgebieten. Durch KI-basierte Analyse aller Datenpunkte generieren wir belastbare, auditierbare Daten für das bereits angesprochene ESG-Reporting und identifizieren hiermit gleichzeitig Optimierungspotenziale für unsere Kunden.

Wie steht es um die „Hardware"-Produktstrategie von Bosch Building Technologies?

Thomas Quante: Wir sind auch hier sehr breit aufgestellt und dadurch in einer guten Ausgangslage. Wir bieten Brandschutzsysteme, Sprachalarm, professionelle Audio-Kommunikationssysteme sowie Video-, Alarm- und Zutrittssysteme.

Beim wichtigen Thema KI profitieren wir massiv von einer übergreifenden Zusammenarbeit. „Leverage the power of Bosch" nennen wir das. Wir sorgen schon jetzt für herausragende KI-Innovationen und tun das auch weiterhin. Nehmen wir zum Beispiel den Bereich Brandschutz und unser Produkt Aviotec…

…Ihre videobasierte Brandfrüherkennung.

Thomas Quante: Genau. Damit gehen wir schon jetzt weit über die regulatorischen Regelungen hinaus. Ein weiteres Beispiel aus dem Bereich Videosysteme: Denken Sie an die Security-Operatoren und ihre enorm herausfordernde Arbeit, bei der Überwachung den Blick auf das Wesentliche zu behalten. Zu viele Falschalarme können hier leicht für eine Desensibilisierung sorgen. Unsere KI-gestützten Systeme helfen hingegen, die wirklich relevanten Dinge zu erkennen und so für eine effiziente Sicherung von Gebäuden oder Perimetern zu sorgen.

An dieser Stelle sei erwähnt, dass Bosch Building Technologies beim „GIT System Test Video Analytics 2022" im Wettbewerb mit namhaften Marktbegleitern sehr gut abgeschnitten hat. Die KI-basierte Videoanalyse mitsamt den Kameras arbeiteten hervorragend…

Thomas Quante: …was mich natürlich nicht überrascht. Genau deswegen vertrauen unsere Kunden in so vielen unterschiedlichen Projekten auf uns, auch ganz besonders in vielen Objekten der kritischen Infrastruktur.

Für ambitionierte Projekte und Vorhaben braucht es engagierte Leute – was tut Bosch für die Unternehmenskultur, für das Miteinander aller Kolleginnen und Kollegen?

Thomas Quante: Das ist für uns schlichtweg das entscheidende Thema für die Sicherung unserer Zukunft. Wir wollen in der Branche gerade auch bei den jungen Talenten immer das bevorzugte Unternehmen sein – egal ob wir mit anderen Großunternehmen oder mit Mittelständlern im sportlichen Wettbewerb stehen. Wir haben wirklich eine Menge zu bieten, vor allem einen tollen Purpose, Gebäudelösungen für ein besseres Leben. Wir unterhalten Kooperationen mit Universitäten im In- und Ausland und veranstalten Hackathons. Eine Vielzahl digitaler Talente entwickelt bei solchen Events zusammen neue Lösungen für eine bessere Zukunft, wobei wertvolle Kontakte zwischen ihnen und unserem Unternehmen entstehen. Erfreulich ist, dass wir bei diesen Events immer mehr Frauen begrüßen dürfen.

Was bieten Sie außerdem beim Werben um die besten Talente?

Thomas Quante: Sehr viel! Zum Beispiel auch eine hohe Flexibilität, was Arbeitszeit und -ort angeht. Bei uns kann sogar eine gewisse Anzahl von Tagen fern des Heimatstandorts im Ausland gearbeitet werden. Im Mittelpunkt steht auch hier das Wohlbefinden der Menschen, in dem Fall unserer Mitarbeitenden, um letztlich auch bestmögliche Ergebnisse zu erzielen.

Gleichzeitig wollen wir unsere Arbeitsplätze vor Ort so attraktiv wie möglich gestalten, so dass Mitarbeitende auch gerne wieder physisch zusammenkommen. Denn im direkten Kontakt entstehen oftmals die besten Ideen. Live zu erleben ist das übrigens auch hier, auf der Bosch Connected World. Die Gespräche, Ideen und Verbindungen, die sich hier ergeben, sind durch nichts zu ersetzen.

Gestatten Sie uns zuletzt eine private Frage: Wie gestalten Sie Ihre sicher spärlich bemessene freie Zeit, um wieder Kraft zu tanken?

Thomas Quante: (lacht) Ich bin nun seit jetzt 28 Jahren „beim Bosch" und genieße es noch immer. Privat verbringe ich gerne Zeit mit meiner Frau und meinen beiden Töchtern. Außerdem gehe ich gerne mit meinem Hund an die frische Luft. Mehr brauche ich nicht.

Vielen Dank für das Gespräch.

Bosch Building Technologies
Grasbrunn
Tel.: +49 89 6290-0
info.service@de.bosch.com
www.boschbuildingtechnologies.com

TITELTHEMA

Es braucht fast nur ein Lächeln…

Interaktionslose Zutrittskontrolle: Abus geht die nächsten innovativen Schritte

Bereits seit 100 Jahren befasst sich Abus mit dem Thema Zutrittskontrolle – und immer noch findet der Sicherheitsspezialist reichlich Potential für ganz neue Möglichkeiten und Weiterentwicklungen. Wie so oft, sind konkrete Kundenwünsche der Ausgangspunkt immer weiterer Innovationen. Abus lässt ihre Ideen und Bedürfnisse in konkrete Projekte einfließen, um die perfekte Lösung zu finden. Die Befragten betonen dabei regelmäßig und einhellig einen zentralen Wunsch: den interaktionslosen Zutritt.

Regional setzt man auf die Alarmanlage Secoris von Abus Security Center

In vielen Lebensbereichen wurden in jüngerer Zeit Technologien optimiert – das Auto lässt sich etwa mit dem Smartphone öffnen, der Zugang zum Handy funktioniert per Gesichtserkennung reibungslos. Nur an der Tür ist diese Transformation noch nicht recht angekommen. Die Abus Produktentwickler arbeiten bereits seit vielen Jahren daran, dies zu ändern.

Interaktionslose Türöffnung

Auf der Security 2016 stellte Abus erstmals seine Vision einer entsprechenden Sicherheitslösung vor. Seitdem beschäftigt sich das Unternehmen kontinuierlich mit der Optimierung der Technik – bis es sechs Jahre später das funktional ausgereifte Ergebnis auf der Security in Essen und der Light & Building vorstellen konnte. Die überwältigende Resonanz machte deutlich, dass die Technologie genau den Vorstellungen des Kundenstammes entsprach.

Das Terminal ermöglicht eine interaktionslose Türöffnung mittels Gesichtserkennung. Hierfür nutzt das Gerät eine 2-MPx-Dual-Kamera (optisch und IR) für eine sicherere und zuverlässigere Erkennung. Wer will, kann sich auch für eine Mehrfachauthentifikation per Gesicht, Pin oder Karte entscheiden.

Dazu kommen sämtliche Funktionen einer Videotürsprechanlage. Das innovative 7-Zoll-Touch-Display am Gerät selbst dient dabei als Interaktions- und Informationsebene. Das Gerät ist IP65-wettergeschützt.

Kein umständliches Authentifizieren

In gewerblich geprägten Kontexten kann das Gerät optimal zur Zutrittsgewährung genutzt werden. An zentralen Türen brauchen sich berechtigte Personen nicht mehr erst umständlich an den Lesern zu authentifizieren. So kann ein schnellerer Personenfluss gewährleistet werden – und zwar, ohne Sicherheit zu verlieren, denn es erhalten trotzdem nur berechtigte Personen Zutritt zu den entsprechenden Bereichen.

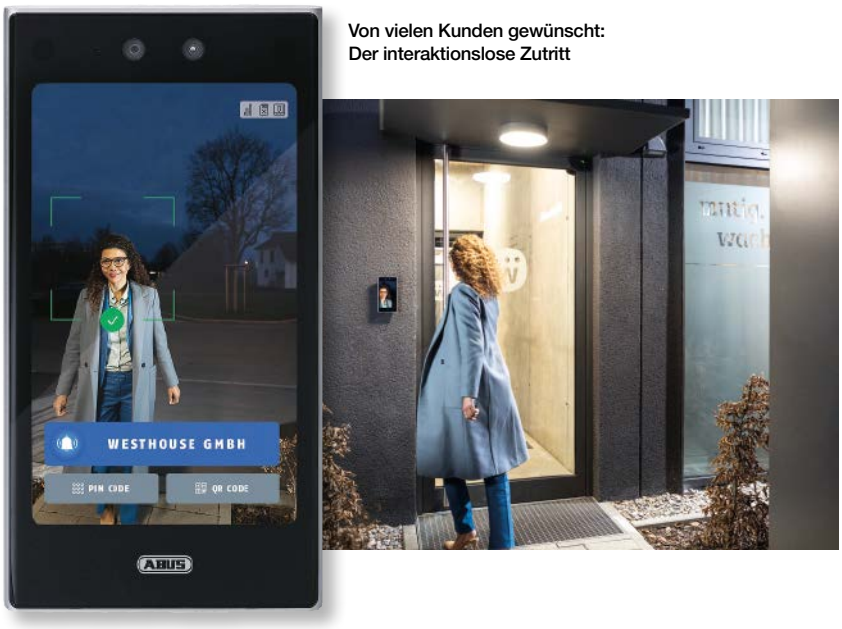
Das Gerät eignet sich auch sehr gut für die Zutrittslösung kritischer Bereiche. So kann beispielsweise unter Berücksichtigung der jeweils gültigen Zugangsregelungen zu bestimmten definierten Bereichen die Zutrittsgewährung auf Personen beschränkt werden, die z. B bestimmte Schutzkleidung tragen.

Auch im gewerblichen Kontext ist das System als Videotürsprechlösung einsetzbar. Sie kann auch als großes Info-Display genutzt werden – zur Darstellung der Öffnungszeiten, des Angebotsumfangs, etc. – auch in Form einer Slide-Show.

Das Einlernen des Systems geht einfach und bequem vonstatten: Es beansprucht am Gerät selbst keine 30 Sekunden. In einem größeren Set up mit mehreren Nutzern können auch Fotos über die Weboberfläche hochgeladen werden und die Daten und Berechtigungen verwaltet werden. Das Gerät ermöglicht es bis zu 10.000 Personen zu verwalten. In einem Netzwerk können die Daten auch auf mehrere Terminals übertragen werden.

Ist das denn sicher?

In den Nutzerstudien von Abus kam erwartungsgemäß immer wieder das Thema Sicherheit auf. Gerade dann, wenn es um die eigenen vier Wände geht, zeigen sich



Von vielen Kunden gewünscht: Der interaktionslose Zutritt

© Bilder: Abus Security Center

Einfach durchgehen! Das Abus Terminal

- Berührungsfreie Türöffnung
- Blitzschnelle Nutzererkennung
- Kein Schlüsselvergessen mehr
- Kombination von verschiedenen Erkennungstechnologien zur Steigerung der Sicherheit (Gesichtserkennung, Pin-Code, Desfire Karte)
- Einfache Nutzerverwaltung und Einlernenprozess innerhalb von 30 Sekunden
- Klingel- und Videotürsprechfunktion
- Abus Link Station App-Anbindung und Kompatibilität zu Abus-Kameras und Rekordern
- Zuverlässige Erkennung auch von Kindern und bei Dunkelheit sowie bei Gegenlicht

> „Wir haben es bei Abus seit fast 100 Jahren mit Schlüsseln zu tun. Da braucht es schon einiges an Vorstellungskraft für dieses nächste ‚Big thing' der Schließtechnik – die Tür mit einem Lächeln zu öffnen. Auch wenn dieser Mehrwert erst einmal buchstäblich nicht greifbar erscheint: Wer es einmal erlebt hat, will niemals mehr anders zur Tür hereinkommen!"

Ralph Leute, Portfoliomanager Abus Security Center

Fortsetzung auf Seite 23 ▶

5 Fragen an …

Abus Security-Center-Geschäftsführer Martin Bemba und Robert Tomic

GIT SICHERHEIT: Herr Bemba, Herr Tomic, Abus hat das neue Jahr mit gewohnt innovativem Schwung begonnen. Auf der Agenda stehen Neuentwicklungen vor allem bei Zutrittskontrolle und Einbruchmeldeanlagen – aber durchaus mit gemeinsamem Nenner...?

Martin Bemba: Wir wollen an die Entwicklungen der letzten Jahre anknüpfen und unsere Systemlandschaft kontinuierlich ausbauen. Unsere Roadmaps sind in allen Produktbereichen gut gefüllt und wir freuen uns sehr darauf unseren Kunden wieder viele neue und innovative Produkte und Lösungen anbieten zu können. Wir haben die vergangenen Monate gut genutzt und intensiv mit unseren Kunden gesprochen. Für uns ist Kundennähe besonders wichtig, um unsere Produkte nicht an den Marktbedürfnissen vorbei zu entwickeln. Und eines der großen Bedürfnisse ist eben der gemeinsame Nenner: die Systemintegration und Interaktion der Gewerke. Gerade für unsere Zutrittskontroll-, Einbruchmelde- und Videosysteme bietet sich das perfekt an. Unsere Kunden erleben heute die gute und kontinuierliche Arbeit der letzten Jahre und erhalten Lösungen aus einer Hand. Darüber hinaus werden wir unsere Systeme auch in diesem Jahr mit vielen neuen Produkten und Funktionalitäten anreichern.

Martin Bemba, Vorsitzender der Geschäftsführung von Abus Security Center

Um nur einige Highlights zu nennen: Mit dem neuen Access-on-card-System Tectiq werden wir einen wichtigen Baustein im Portfolio der Zutrittskontrolle liefern. Das Secoris-System wird um die neue Funktechnologie und Bedienfelder erweitert. Im Video- und Zutrittsbereich freuen wir uns auf das neue Face Access Terminal.

Beginnen wir mit dem neuen Zutrittssystem. Hier steht ja vor allem das interaktionslose Nutzen von Türen im Vordergrund?

Robert Tomic: Eine Interaktion zur Authentifizierung eines Nutzers muss in Zukunft nicht mehr zwingend erforderlich sein... Die Authentifizierung ohne ein elektronisches Zutrittsmedium gewinnt im Markt immer mehr an Interesse und Beliebtheit. Gerade Produkte, die auf biometrischen Technologien basieren, sind im Trend und werden häufig nachgefragt. Solche Produkte sind schon länger vorhanden und werden kontinuierlich weiterentwickelt und die Zuverlässigkeit und Reaktionsgeschwindigkeit verbessert. Auch Abus beschäftigt sich schon länger mit dieser Technologie. Wir wollen mit unserer neuen Lösung dem Wunsch des Marktes nachkommen und eine Lösung per Gesichtserkennung (Face Access) anbieten.

Martin Bemba: Unser Face-Access-Terminal ist bereits heute mit Produkten unseren Moduvis Intercom kompatibel. Das Gerät soll aber nicht nur eine zentrale Rolle bei der Öffnung von Türen spielen, sondern perspektivisch auch in unsere Einbruchmelde- und Zutrittskontrollsysteme integriert werden. Wie sie sehen, denken wir auch hier ganzheitlich integrativ und bringen unsere Systeme immer näher zusammen.

Die Einbruchmeldeanlage Secoris, Sie erwähnten es bereits, ist eine leistungsstarke Einbruchmeldeanlage für Unternehmen mit bis zu 200 Nutzern?

Robert Tomic: Die Secoris ist für Abus die neue und zentrale Alarmplattform für den professionellen Einbruchschutz. Als Draht- bzw. Hybridsystem nach EN 50131 Grad 2 und 3 können wir damit alle Anforderungen an eine Alarmanlage problemlos abdecken. In Kürze werden wir das Secoris System um ein neues Funksystem mit modernster Funktechnologie ergänzen, die unseren Kunden fortan höchste Flexibilität bei der Installation, bei höchster Sicherheit bietet. Die Benutzerverwaltung erfolgt bequem in unserer Abus-Cloud, der Zugriff und Bedienung kann über die zugehörige Secoris-App erfolgen. Die Secoris Alarmplattform werden wir kontinuierlich weiterentwickeln. Auch hier setzen wir auf Integration: Eine Einbindung in Gebäudeautomation ist ebenso vorgesehen wie die native Integration unserer Zutrittskontrollsysteme. Mit der Secoris bieten wir damit einen Rundumschutz an.

Robert Tomic, Geschäftsführer Abus Security Center

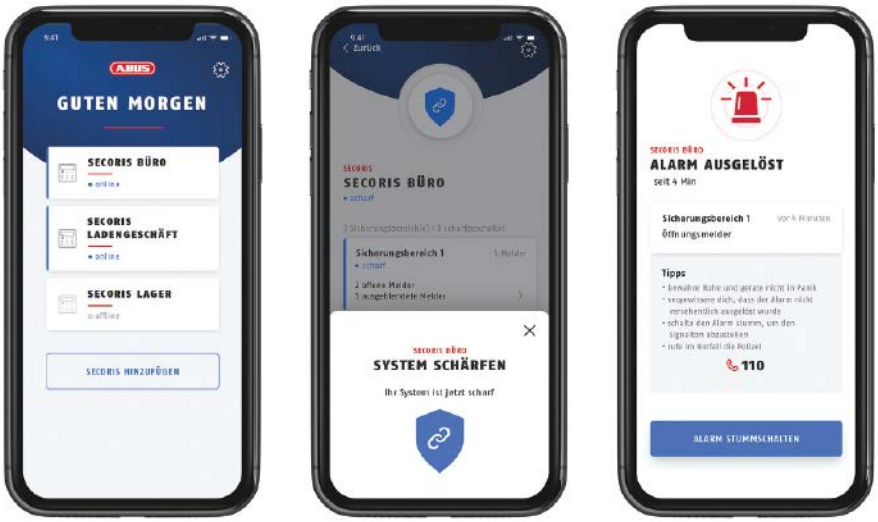
Wo liegen die Unterschiede zur Secvest?

Robert Tomic: Mit der Secvest haben wir eine Funkalarmanlage, die ideal für kleine private und gewerbliche Objekte geeignet ist. Mit der Secoris gehen wir nun einen Schritt weiter. Hier liegt der Fokus auf kleine bis mittlere gewerbliche Objekte, wo die Anforderungen und auch Vorteile eines Hybridsystems – also Draht in Kombination mit Funk – ausgespielt werden können.

Für wann ist jeweils die Markteinführung in der besprochenen Form geplant?

Martin Bemba: Die Alarmplattform Secoris haben wir ja bereits 2022 erfolgreich in den Markt eingeführt. Das neue Funksystem wird im zweiten Quartal des Jahres verfügbar sein. Das Face Access-Terminal wird voraussichtlich im dritten Quartal erhältlich sein. ●

Fortsetzung von Seite 21 ▶



◀ Die Alarm-View zeigt den bei Alarm ausgelösten Sicherungsbereich samt Meldergruppe und Handlungsempfehlung

Kunden verständlicherweise wenig kompromissbereit. Die Gesichtserkennung erfolgt mittels einer dualen Kamera, so kann ein Liveness-Check erfolgen. Dabei wird überprüft, ob sich überhaupt um eine lebende Person, oder nur ein Foto, das jemand vor die Kamera hält. Für hochsensible Zutrittsbereiche kann die Doppelverifikation das Sicherheitslevel noch weiter erhöhen – etwa durch das Vorhalten eines Identmediums über Mifare Desfire.

Die Gesichtsdaten werden verschlüsselt auf dem Gerät auf einem verschlüsselten Chip gespeichert und verlassen das Gerät nicht. Das Gerät muss auch nicht online sein, sondern kann stand alone als Türöffner oder in einem lokalen Netzwerk als Videotürsprechstation betrieben werden. Damit ist sichergestellt, dass persönliche Daten sicher sind.

Mehrwert für den Kunden

Eine der größten Überraschung der Analyse war für Abus, dass die begeistertsten Nutzer Frauen sind. Man ging zunächst davon aus, dass das Produkt besonders bei technikaffinen Männern punkten würde. In Live-Tests und bei Feldtest hat sich aber herausgestellt, dass das Produkt gerade auch bei Frauen sehr gut ankommt, weil das Kramen nach dem Schlüssel in der Tasche somit endlich der Vergangenheit angehört. Frauen spielen bei einer solchen Kaufentscheidung eine entscheidende Rolle spielen – für Abus ein weiterer klarer Vorteil des neuen Systems.

Abus hat das Device auf der Security und L&B vorgestellt. Das Kundenfeedback sei überwältigend gewesen, so das Unternehmen. Es war spürbar, dass die Technologie die Kundenwünsche genau erfüllt: Wer das System einmal erlebt hat, möchte nie mehr anders zur Tür hereinkommen. ●

Abus Security Center GmbH & Co. KG
Affing
Tel.: +49 8207 959 90 0
sales@abus-sc.com
www.abus.com

Die Alarmanlage Secoris von Abus ist für Anwendungen in Büroumfeldern und für Gewerbeobjekte

Draht oder Funk? Die Antwort lautet: Ja! …

… denn die Alarmanlage Secoris von Abus Security Center kann beides: Das leicht bedienbare Gerät ist die leistungsstärkste ihrer Art von Abus und wird vom Facherrichter installiert und gewartet. Ausgelegt ist sie für Anwendungen in Büroumfeldern und für Gewerbeobjekte und kommt mit der für die Versicherung vieler Betriebe wichtigen EN-Grad-2-Zertifizierung – mit Alarm- und anderen Sicherheitsfunktionen vor allem zum Schutz vor Einbruch, Feuer oder Wasserschäden.

Mit den digitalen Schließ- und Zutrittskontrollsystemen des Herstellers ist die Anlage kompatibel – und mit bis zu zehn IP-Kameras kann der Anwender alarmauslösende Ereignisse visuell verifizieren. Konfigurieren lässt sich die Alarmanlage für bis zu 200 Nutzer bzw. 200 einzeln identifizierbare Meldergruppen, 50 Bus-Komponenten und 20 Sicherungsbereiche.

Die Alarmanlage ist variabel für den Kunden konfigurierbar und erweiterbar – per Funk oder Draht oder in Kombination aus beidem. Volle Flexibilität bei der Zuordnung von Berechtigungen, automatisierten Zeitplänen, etc. ist ebenfalls leicht bedienbar gewährleistet.

Wie es der heutige Nutzer es erwartet, lässt sich die Alarmanlage mit digitalen Endgeräten wie Handy und Tablet mobil und in Echtzeit bedienen und steuern – von bis zu 200 App-Nutzern mit ihren persönlichen Berechtigungen, die mit Hilfe einer eigenen Web-Schnittstelle angelegt werden. Ihnen werden die einzelnen Funktionen der App mit einem Onboarding-Assistenten bedienerfreundlich zugänglich gemacht. Sie öffnet sich sicher per Passwort, Fingerabdruck oder Gesichtserkennung.

Soweit der Kunde dies wünscht, kann er sich per Abus-Cloud und Secoris-Portal bei der Verwaltung, Ferndiagnose und Wartung vom Fachbetrieb unterstützen lassen.

◀◀ zurück zum Inhaltsverzeichnis

© Bilder: SimonsVoss/Bernhard Lehn

SCHLIESSSYSTEME

Bereit für New Work

Deutschlands größte IHK setzt auf digitale Schließtechnik

Die Industrie- und Handelskammer (IHK) für München und Oberbayern ist mit mehr als 410.000 Mitgliedsunternehmen die größte IHK Deutschlands. Die beiden Standorte in der bayerischen Landeshauptstadt sowie die Geschäftsstellen in Ingolstadt und Weilheim sind komplett mit digitaler Schließtechnik von SimonsVoss ausgestattet – eine Maßnahme, die Sicherheit, Flexibilität und Komfort für Mitarbeitende, Mitglieder und Kunden integriert.

Oberstes Ziel der IHK ist nach eigenem Bekunden, „beste Rahmenbedingungen für den nachhaltigen wirtschaftlichen Erfolg der gewerblichen Unternehmen in München und Oberbayern zu schaffen." Dieser vielfältige Anspruch stellt eine tägliche Herausforderung für die rund 440 Beschäftigten dar, allein am Campus in der Münchner Orleansstraße zählt man bis zu 3.000 Kunden am Tag. Mit den Häusern A bis D, in denen viele IHK-Mitarbeiter und Seminarräume der IHK-Akademie untergebracht sind, ist dies der flächenmäßig größte Standort, gefolgt vom Stammsitz im historischen Gebäude an der Max-Joseph-Straße. Dazu kommen die Geschäftsstellen in Rosenheim, Ingolstadt, Weilheim und Mühldorf sowie eine Außenstelle der Akademie in Feldkirchen-Westerham.

Matthias Schölzel, Referatsleiter Gebäudemanagement, erklärt: „Insgesamt sind es rund 70.000 m² Fläche, die wir betreuen." Zu den Aufgaben zählt auch der Bereich Zutrittssteuerung, der inzwischen nahezu komplett auf digitale Schließtechnik umgestellt ist. Fast 1.200 digitale Schließzylinder des Systems 3060 von SimonsVoss Technologies sind aktuell in den Gebäuden der IHK im Einsatz, dazu über 100 elektronische SmartHandle-Türbeschläge sowie mehrere hundert Aktiv-Transponder unter anderem für die gut 440 Mitarbeitenden.

Premiere in Weilheim

Der Einstieg in das digitale Schließzeitalter bei der IHK für München und Oberbayern fand 2015 in Weilheim statt. „Das war unser Premierenstandort, hier sind wir mit einer Testanlage samt Leihzylindern gestartet, welche die mechanische Schließanlage ersetzt hat", erinnert sich Matthias Schölzel. Per Mock-up-Demonstration hat er die Beschäftigten vor Ort mit der Nutzung der Digitaltechnik vertraut gemacht, ein Prozess, „der durchaus Zeit in Anspruch genommen hat, weil das gesamte

◀◀ zurück zum Inhaltsverzeichnis

◀ Stammsitz der IHK München und Oberbayern in der Münchener Max-Joseph-Straße

Handling neu war." Geliefert, montiert und gewartet wird die digitale Schließtechnik in den Gebäuden der IHK seitdem durch den Fachhandelspartner Tobler aus München.

Schlüsselverlust forciert Systemwechsel

Entsprechend gingen die IHK-Verantwortlichen auch am Stammsitz in der Max-Joseph-Straße vor. 2011 begann eine Komplettsanierung dieses über 100 Jahre alten Gebäudekomplexes, der schon immer die IHK für München und Oberbayern beherbergt hat. Für rund sieben Jahre mussten die Beschäftigten in ein Mietobjekt in der Balanstraße umziehen. Hier gab es ein Ereignis, das letztlich die generelle Umstellung auf digitale Schließtechnik bei der IHK deutlich beschleunigt hat. „Wir hatten den Verlust eines sehr weit oben in der Schließhierarchie angesiedelten mechanischen Schlüssels zu beklagen und haben so die Risiken aus erster Hand erlebt", berichtet Matthias Schölzel. So wurde das Gefahrenpotential, das mit einer mechanischen Schließanlage verbunden sein kann, mehr als deutlich. „Deswegen haben wir im Zuge der Sanierung die Liegenschaft Max-Joseph-Straße gleich auf digitale Schließtechnik umgestellt."

In den Campus-Gebäuden an der Orleansstraße wurde 2019 wie beim Standort Weilheim innerhalb von einer Woche die mechanische durch eine digitale Schließanlage ersetzt. Dieser Schritt steht in der IHK-Geschäftsstelle Rosenheim noch aus. In Mühldorf sind die IHK-Räumlichkeiten im dortigen Landratsamt gemietet, daher nutzt man aktuell das dort vorhandene Schließsystem des Vermieters.

Online- und Offline-Varianten

Das Organisations- und Verwaltungsprinzip der digitalen Schließtechnik ist standortbezogen aufgebaut. „Zu meiner Abteilung gehören für jedes Gebäude verantwortliche Teamleiter, die sich um die Zutrittsteuerung kümmern", erläutert Matthias Schölzel, „wir verwenden dabei für die Max-Joseph-Straße und die Campus-Gebäude A, B und C die Online-Variante der 3060-Anlage, für Gebäude D und die Geschäftsstellen die Offline-Version."

Mit der umfassenden Online-Vernetzung kann die IHK das ganze Leistungsspektrum des Systems 3060 nutzen. Die Doppelknaufzylinder sind je nach Zugangsart mit unterschiedlichen Features versehen, wie etwa Zutrittskontrolle, Zeitzonensteuerung und Protokollierung, als feuerhemmende Version in Brandschutz- und Notausgangstüren, mit Antipanikfunktion oder als wetterfeste Variante in Außentüren. Auch die Bedienung ist jeweils auf die Eingangssituation angepasst: Zylinder können von außen und innen mit dem Transponder geöffnet werden. Bei vielen Bürotüren ist die Nicht-Elektronikseite fest eingekuppelt, so dass sie von innen ohne Transponder bedienbar sind. Eine besondere Herausforderung stellten einige historische Türen im sanierten Gebäude Max-Joseph-Straße dar – hier waren beispielsweise Zylinderlängen von bis zu 260 mm notwendig, bei deren Einsatz auch die Denkmalschutzbehörde keine Einwände hatte.

Sicherheit auch bei Transponder-Verlust

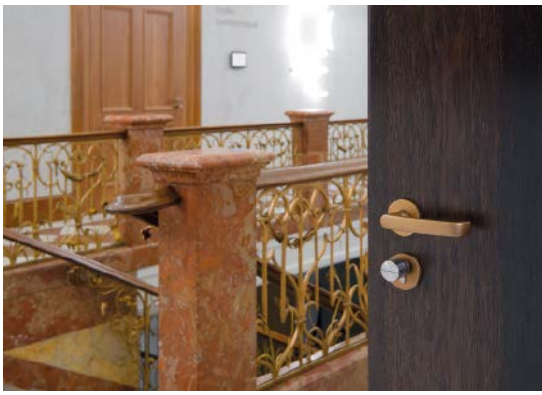
Die Locking-System-Management-Software (LSM) und sämtliche Schließungen werden per Funk und über Router verbunden, was den Datenaustausch in Echtzeit gewährleistet. Die Vorteile liegen im zentralen Management an jedem Standort, den vielen Funktionen und einer deutlich erhöhten Sicherheit. Bei Verlust eines Transponders kann der jeweilige Teamleiter sofort reagieren, er kann Schließungen in Echtzeit programmieren und hat stets den Überblick über den aktuellen Status der betreffenden Anlage. Er selbst besitzt die Schließberechtigungen für alle Zugänge seines Verantwortungsbereiches, darunter sind dann die weiteren Ebenen im jeweiligen Gebäude angeordnet.

Da im Campus-Gebäude D insgesamt deutlich weniger Türen vorhanden sind und auch das Kostenargument Berücksichtigung finden sollte, wurde hier und für die externen Geschäftsstellen die Offline-Version des 3060-Systems gewählt. Die Programmierungen werden hier ebenfalls in der LSM-Software erstellt, die Daten aber auf einem tragbaren Programmiergerät zur betroffenen Schließung gebracht. Alternativ können die Teamleiter die Identifikationsmedien entsprechend programmieren, was häufig eine einfachere Möglichkeit darstellt.

SmartHandle-Türbeschläge als Ergänzung

In der gesamten IHK München und Oberbayern kommen ausschließlich Aktiv-Transponder als Schließmedien zum Einsatz. „Das hat sich bewährt", erklärt Matthias Schölzel, „und wir haben die Transponder zusätzlich mit RFID-Chips ausstatten lassen, so dass die Mitarbeitenden beispielsweise die Multifunktionsgeräte individuell bedienen können, etwa wenn sie vertrauliche Unterlagen ausdrucken wollen. Genauso bietet das System die Möglichkeit einer Bezahlfunktion in der Kantine und damit reichlich Komfort für unsere Beschäftigten."

Komfort und Flexibilität waren wesentliche Gründe für die Integration von insgesamt über 100 digitalen SmartHandle-Türbeschlägen von SimonsVoss in die IHK-Schließtechnik. Der weitaus größte Teil wurde in den Campus-Gebäuden A-D eingebaut. Ihr Nutzen zeigt sich etwa bei der Belegung der Prüfungsräume. Hier sind nicht nur die eigenen IHK-Experten im Einsatz, sondern je nach Themengebiet und Lehrgang auch externe Prüfer, Sachverständige oder Gutachter. Sie erhalten am Empfang



Fast 1.200 digitale Schließzylinder des Systems 3060 von SimonsVoss sind derzeit in den Gebäuden der IHK im Einsatz

In der gesamten IHK München und Oberbayern kommen ausschließlich Aktiv-Transponder als Schließmedien zum Einsatz

Die Transponder wurden zusätzlich mit RFID-Chips ausgestattet, so dass die Mitarbeiter beispielsweise die Multifunktionsgeräte individuell bedienen können, etwa wenn sie vertrauliche Unterlagen ausdrucken wollen

Bitte umblättern ▶

Die Doppelknaufzylinder sind je nach Zugangsart mit unterschiedlichen Features versehen, darunter etwa Zutrittskontrolle, Zeitzonensteuerung und Protokollierung, als feuerhemmende Version in Brandschutz- und Notausgangstüren, mit Antipanikfunktion oder als wetterfeste Variante in Außentüren

Mit der umfassenden Online-Vernetzung kann die IHK das ganze Leistungsspektrum des Systems 3060 nutzen

gegen Unterschrift ihren für den jeweiligen Prüfungsraum gültigen Transponder und können den Raum über den SmartHandle-Beschlag öffnen und auch wieder verriegeln. „Durch diese Konstellation können wir vom Gebäudemanagement unter Berücksichtigung anwendbarer datenschutzrechtlicher Vorgaben für jeden Raum einzeln nachvollziehen, wer ihn wann und wie lange genutzt hat“, erklärt Matthias Schölzel.

New Work – neue Herausforderungen

Generell ist der Referatsleiter Gebäudemanagement vor allem mit der Nutzungsbreite der digitalen Schließtechnik in den IHK-Liegenschaften sehr zufrieden. Die Technik bewährt sich vor allem bei den hohen Besuchsfrequenzen und durch die Möglichkeiten, den Nutzungsumfang exakt auf die jeweilige Gebäudesituation zuschneiden zu können. So wird die IHK künftig als Vermieter aktiv, da „New Work“ und Home-Office-Regelungen auch für die IHK Veränderungen in der Arbeitsorganisation und frei werdende Räume mit sich bringen. Die Mieter nutzen die digitale Schließtechnik in gleicher Art und Weise, auch Programmierung und Verwaltung der Anlage verbleiben bei den IHK-Teamleitern.

„Wir können die digitale Schließanlage sehr schnell an die New-Work-Anforderungen anpassen“, so Matthias Schölzel, „früher hat ein Mitarbeiter einen Raum dauerhaft genutzt, heute sind im selben Raum fünf Mitarbeitende zu unterschiedlichen Zeiten aktiv, entsprechend variabel muss die Zutrittssteuerung sein.“ Möglich ist künftig auch der Einsatz des neuen digitalen Schließzylinders DCAX von SimonsVoss. Die neuen modularen Zylinder sind abwärtskompatibel und damit auch im 3060-System verwendbar. Sollte einer der bestehenden Zylinder einmal ausgetauscht werden müssen, kann also auch punktuell mit dem neuen System nachgerüstet werden. ●

SimonsVoss Technologies GmbH
Unterföhring
Tel.: +49 89 99 22 8 0
marketing-simonsvoss@allegion.com
www.simons-voss.com

Flexible Arbeitsplätze dank iLoq und DeskNow

Die Integration der Zutrittsmanagementlösung von iLoq und der Workspace-Management-Plattform von DeskNow schafft flexible Arbeitsplätze. Sie ermöglicht einen schnellen und effizienten Zugang zu gemeinsam genutzten Arbeitsbereichen in ganz Europa. DeskNow wurde 2020 in Deutschland gegründet und ist eine Online-Workspace-Management-Plattform, um Büros zu verwalten, diese buchbar zu machen und jede Art von Arbeitsplatz in ganz Europa zu digitalisieren. Die mehrsprachige Plattform ist rund um die Uhr über die Website oder eine App des Unternehmens verfügbar. Der Hauptvorteil der Integration besteht darin, dass sie Nutzern rund um die Uhr Zugang zu Räumen bietet. Sicherheit hat daher eine hohe Priorität, da Vermieter sicherstellen müssen, dass nur autorisierte Personen zur richtigen Zeit Zugang zu den richtigen Orten haben.

© iLoq

iLoq und DeskNow schaffen gemeinsam flexible Arbeitsbereiche

www.iloq.com

Zweimal die Bestnote „sehr gut“ für Feig-Azubis

Da gut ausgebildete Fachkräfte auf dem Arbeitsmarkt schwer zu finden sind, engagiert sich Feig Electronic als Ausbildungsbetrieb. Zahlreiche Talente vor allem aus der heimischen Region wurden seitdem ausgebildet und vielfach als Mitarbeiter übernommen. 2022 gingen aus den Feig-Azubis zwei Ausbildungs-Champions hervor. Jannik Halm und Adrian Huckwitz sind diese beiden Ausbildungs-Champions. Beide haben ihre zweijährige Ausbildung zum Industrieelektriker für Geräte und Systeme mit der Bestnote „sehr gut“ abgeschlossen und erhielten deshalb von der Industrie- und Handelskammer Limburg die Auszeichnung „Ausbildungs-Champion 2022“. Auf ihren Lorbeeren ausruhen wollten sich jedoch beide nicht: Jannik Halm als auch Adrian Huckwitz wählten die weiterführende Ausbildung bei Feig zum Elektroniker für Geräte und Systeme, die weitere 1,5 Jahre dauern wird.

© Feig

Jannik Halm (l.) und Adrian Huckwitz bei der Übergabe der Auszeichnung zum Ausbildungs-Champion 2022

www.feig.de

◄◄ zurück zum Inhaltsverzeichnis

Dreh-Kipp-Fensterbeschlag ActivPilot

Das Beschlagsystem Winkhaus ActivPilot eröffnet komfortable Spielräume bei der Herstellung schwerer Fenster. Denn dessen starke Bandseite trägt ohne Zusatzbauteile bis zu 150 kg Flügelgewicht. Ihre cleveren technischen Details erzielen eine beeindruckende Wirkung: Die Lagerteile der Bandseite sind aus massivem Stahl gefertigt. Um die Belastung durch die höheren Gewichte besser zur verteilen und die Abstützung auf dem Blendrahmen zu verbessern, sind die Auflageflächen groß. Zudem ist das Ecklager am unteren Ende länger ausgeführt. Das optimiert die Lastabtragung bei schweren Flügeln.

Diese stabile Lösung punktet ästhetisch wie funktional: Die hochbelastbaren Stahllager eignen sich auch für schmale Blendrahmen. Die Schraubenköpfe sind im montierten Fenster nicht sichtbar, weil sie vom Scherenband und Flügellager abgedeckt werden. Die leistungsfähige Bandseite ist nach den Prüfkriterien der neuen DIN EN 18126-8:2017 H3 getestet. Mit nur drei Verschraubungen des Scherenlagers in der Armierung ist es beim Test gelungen, 20.000 Öffnungs- und Schließzyklen mit Flügelgewichten bis 130 Kilogramm zu durchlaufen und damit den Richtlinien der Gütergemeinschaft Schlösser und Beschläge zur Verschraubung von lastabtragenden Beschlagteilen bei Dreh-Kipp-Fenstern (TBDK) gerecht zu werden.

Mit einer vierten Verschraubung des Scherenlagers in die Stahlarmierung ist eine Tragkraft von bis zu 150 kg unter den gleichen Bedingungen möglich. Deswegen kann der Hersteller auf eine Sonderbandseitenlösung mit mehr Verschraubungen verzichten. Alle gängigen Kunststoff-Fenster sowie Holz- und Aluminium-Fenster mit 16 mm Flügelbeschlagnut sind damit realisierbar. Das gilt auch für wirkungsvolle Einbruchschutzfunktionen (bis RC3). Zur Auswahl stehen zwei Flügellagervarianten: Eine wird als Zapfenausführung zur Verschraubung in den Flügelüberschlag angeboten, die andere als Falzbandausführung. Das Falzbandflügellager ist einteilig gerollt und somit komplett aus Stahl. So kann es deutlich höhere Flügelgewichte tragen. Auf Wunsch wird es auch mit Pulverbeschichtung in breiter Farbpalette geliefert.

Die Überschlagsflügellager gibt es standardmäßig mit Höhenverstellung, optional sind sie auch mit zusätzlicher Drehhemmung oder mit Anpressdruckverstellung erhältlich. Auch ein nachträglicher Austausch der Lagervarianten ist problemlos, da die Flügellager untereinander identische Schraub- und Zapfenpositionen haben. Das dazu passende Ecklager wird in zwei Varianten angeboten: Die schmale Ausführung (12 mm breit) wird in Kombination mit dem Falzbandflügellager eingesetzt. Das breite (16 mm), gleichfalls rechts/links einsetzbare Ecklager ist für die Kombination mit dem Überschlagflügellager vorgesehen. Für hohe Flügelgewichte steht ein langer Zapfen zur Verfügung, der bis in die Stahlarmierung hineinreicht.

www.winkhaus.de

© Bilder: Winkhaus

Die starke Bandseite von Winkhaus ist stabil und dennoch dezent

Die stabilen Eck- und Scherenlager aus Stahl von ActivPilot Concept tragen ohne Zusatzbauteile bis zu 150 kg Flügelgewicht

Telenet und F24: Öffentliches Warnsystem für Belgien

Telenet und F24 stellen bis 2028 weiter das Warnsystem BE-Alert für die belgische Regierung bereit. Beide Parteien haben gemeinsam die öffentliche Ausschreibung des Föderalen Öffentlichen Dienstes des Inneren in Belgien gewonnen. Telenet und F24 haben eine Komplettlösung für Gemeinden und staatliche Dienste entwickelt, die es ermöglicht, Notfallmeldungen an die Bevölkerung zu versenden. Man freue sich sehr, die Zusammenarbeit mit dem Nationalen Krisenzentrum fortzusetzen, so Geert Degezelle, Vice President bei Telenet Business. Die stetige Weiterentwicklung der Lösung verbessere kontinuierlich die Leistungsfähigkeit von BE-Alert, wie sich bei den Überschwemmungen in Wallonien vor gut eineinhalb Jahren und auch während der Coronakrise gezeigt habe. Telenet war an der Entwicklung des BE-Alert-Systems seit dem Start im Jahr 2016 beteiligt. Die Partnerschaft mit F24 besteht also schon seit einiger Zeit.

www.f24.com

Die GIT SICHERHEIT ist für mich wichtig, weil die aktuellen Informationen und Berichte einen Blick über den Tellerrand ermöglichen und mich stets auf dem Laufenden halten.“

Dr. Peter Burnickl, CEO, Geschäftsführender Gesellschafter, Burnickl Ingenieure Holding GmbH

◄◄ zurück zum Inhaltsverzeichnis

SMART HOMES

Wir brauchen einen Aktionsplan!

Die sichere, inklusive und nachhaltige Stadt als weltweites Ziel

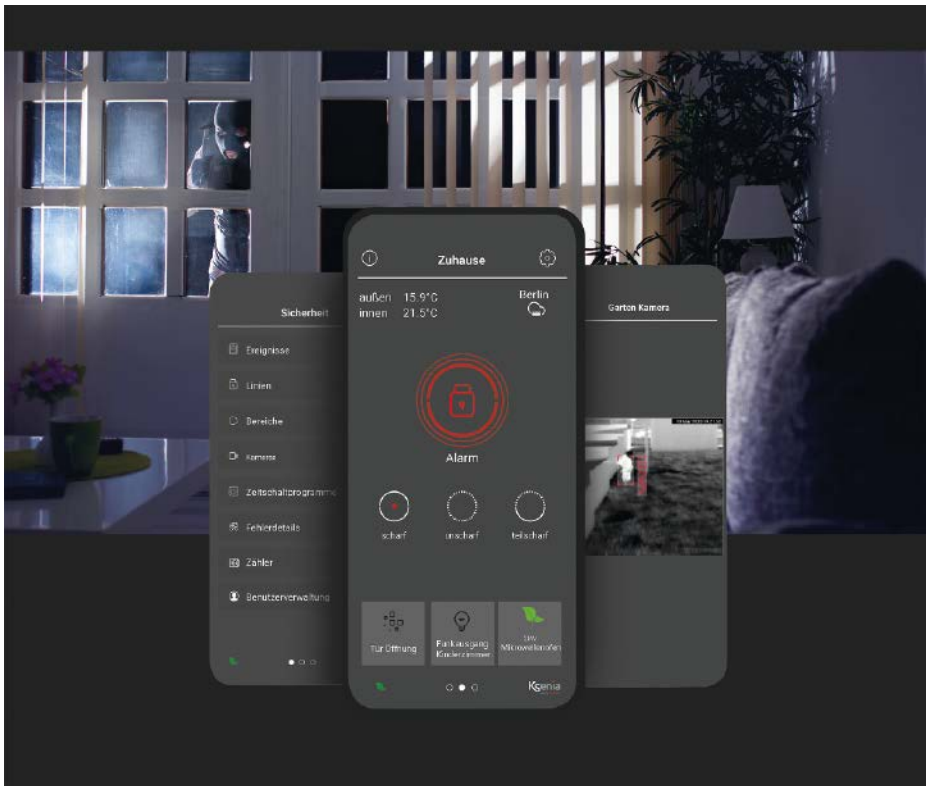
Ksenia Security erkennt in der weltweiten Entwicklung der Städte und deren Nachhaltigkeit ein wichtiges Thema für die Entwicklung ihrer eigenen Lösungen.

Die Urbanisation habe, so stellt Ksenia Security in einem seiner jüngsten Blogs fest, mit den Jahren zu erheblichem wirtschaftlichem, sozialem und kulturellem Wachstum geführt. Städte seien heute die Zentren der Innovation und böten sehr gute Möglichkeiten – gleichzeitig könne man die enormen Einflüsse dessen auf die Umwelt nicht übersehen. Jüngste Statistiken hätten gezeigt, dass der städtische Raum zwar nur drei Prozent der Erdoberfläche in Anspruch nehmen – diese aber für den Verbrauch mehr als der Hälfte der weltweiten Ressourcen und CO_2-Emissionen in die Atmosphäre verantwortlich seien.

Um nun sicherzustellen, dass die Städte künftig weiterwachsen könnten, ohne der Umwelt unwiederbringliche Schäden zuzufügen, sei ein Aktionsplan nötig, um sie sicherer, inklusiver und nachhaltiger zu machen. Die Ziele der Agenda 2030 der Vereinten Nationen seien klar: Zugang zu sicherem Wohnen soll allen Menschen gewährt werden – einschließlich Grundversorgung, eines nachhaltigen Mobilitätssystems, verbesserten Abfallmanagements – bei gleichzeitiger Beachtung des kulturellen und natürlichen Erbes das die Städte zu bieten haben.

Damit diese Ziele erreicht werden können, sei es wichtig, dass die Institutionen ein soziales Nachhaltigkeitsprogramm verfolgten, das sich in Richtung Inklusion und Armutsbekämpfung bewege und für Umweltschutz, insbesondere die Smogvermeidung in den Ballungszentren, sorge.

Dass jeder Einzelne dazu mit einfachen kleinen Maßnahmen bereits etwas beitragen könne, dürfe man nicht vergessen. Beispiele dafür seien die Einschränkung beim Nutzen des Autos, beim Energieverbrauch und die Sorgfalt hinsichtlich des Müllaufkommens.



Hausautomation und Sicherheit von Ksenia

© Ksenia

Nachhaltigkeit im Unternehmen

Ksenia selbst zählt nachhaltiges Handeln zu den Werten, die bereits die Gründung des Unternehmens trugen. Es gehöre zur Unternehmensphilosophie des Hauses, dies auch den Mitarbeitern, Kunden und Lieferanten zu vermitteln – und damit zu einer Gesellschaft beizutragen, die sich stärker an dem Ziel einer grünen Zukunft orientiert. So sei bereits die Firmenzentrale eine regelrechte Nachhaltigkeitsoase – beispielsweise als Produzentin erneuerbarer Energie durch Photovoltaik auf dem Dach.

Man bevorzuge außerdem nachhaltige Mobilitätskonzepte und habe deshalb den Grundsatz „Made in Marche“ (also hergestellt in den italienischen Marken) als Teil der Firmenstrategie festgelegt. Demnach bemüht man sich darum, jede Aktivität in der Region zu tätigen – etwa bei der Auswahl lokaler Zulieferer – um CO_2-Emissionen einzusparen. Außerdem bietet Ksenia seinen Mitarbeitern die Möglichkeit, von zuhause aus zu arbeiten – und man unterstützt eine Gesellschaft für den Umweltschutz in Italien. ●

Ksenia Security SpA
Ripatransone (AP), Italien
Tel.: +39 0735 751646
info@kseniasecurity.com
www.kseniasecurity.com

◄◄ zurück zum Inhaltsverzeichnis

© ABI-Sicherheitssysteme

E-Learning-Portal von ABI

E-Learning-Portal

ABI-Sicherheitssysteme erweitert sein Schulungsangebot um ein E-Learning-Portal. Von der Produktvorstellung für Planer bis hin zur Grundlagenschulung im System MC 1500 für Techniker wird eine große Bandbreite an Themen abgedeckt. Zum Start des E-Learning-Portals im ersten Quartal 2023 stehen circa 30 Online-Trainings zur Verfügung. Die Trainingsinhalte werden fortlaufend ausgebaut. Das E-Learning-Portal bietet unter anderem folgende Vorteile: ortsunabhängiges Lernen, Lerninhalte jederzeit und beliebig oft aufrufbar, individuelles Lerntempo, technische Grundlage und praktische Übungen, Lernkontrolle durch Prüfungsfrage, automatisierte Zertifikate-Erstellung nach erfolgreicher Prüfung und für Geschäftsführer: exklusiver Statistik-Zugang zur Fortschrittskontrolle der Mitarbeiter.

www.abi-sicherheitssysteme.de

Schrank und Spind clever gesichert

Das digitale Schrankschloss SmartLocker AX von SimonsVoss sichert Spinde, Umkleidekabinen oder Depotfächer. Das aus Schloss und Außenleser bestehende SmartLocker AX geht in einigen technischen Details eigene Wege: Der modulare Aufbau ermöglicht eine bohrungsfreie Montage mithilfe eines innovativen Klemmmechanismus durch die in der Regel vorhandene 19-mm-Doppel-D-Stanzung. Auch bei einer Nachrüstung des Schlosses bleibt der Schrank unbeschädigt, ein wichtiger Vorteil z. B. in Mietverhältnissen. SmartLocker AX verzichtet auf einen manuellen Verschluss, die AX-Elektronik arbeitet vollautomatisch: Bei Betätigung eines berechtigten aktiven SimonsVoss Transponders bzw. bei Vorhalten einer berechtigten RFID-Mifare-Karte fährt der motorisierte Riegel automatisch ein- bzw. aus. SmartLocker AX lässt sich in der Riegelpositionierung durch mitgelieferte Adapter an die Anforderungen vor Ort anpassen.

© SimonsVoss

SmartLocker AX von SimonsVoss

www.simons-voss.com

OSS – Die Zukunft der mobilen Zutrittskontrolle

Dom entwickelt gemeinsam mit Hard- und Softwareherstellern Sicherheitsstandards im Bereich der Zutrittskontrolle. Das Unternehmen ist Mitglied der OSS Association (Open Security Standards Association). Dank des OSS Mobile Access Standards wird der mobile Zugang künftig einfacher und bequemer. Der Standard OSS MA definiert jene Schnittstellen, die für die Verwendung eines Smartphones als Schlüssel bzw. Mobile Credential notwendig sind. Das Web-Interface ist hierbei besonders hervorzuheben. Dieses ermöglicht es Anbietern von Software für Zutrittsmanagement, mobilen Zutritt schnell und einfach in ihre Lösungen zu integrieren. Darüber hinaus tun sich jedoch auch zahlreiche Möglichkeiten für Anbieter von web-basierten Lösungen wie zum Beispiel Buchungsplattformen auf.

© DOM

www.dom-security.com

Stefan Dörenbach, Country Manager DACH

VIDEOSICHERHEIT

Wir liefern

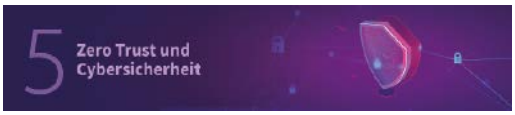
KI, Cloudlösungen und Cybersicherheit im Fokus

Der koreanische Hersteller Hanwha Techwin hat seine weltweite Marktposition in den letzten Jahren kontinuierlich ausgebaut und das Erbe der Samsung-Produkte erfolgreich angetreten. Für die Videosicherheit bietet der Hersteller mittlerweile ein komplettes Angebot von der Kamera, über die Speicherung bis hin zum Videomanagement. GIT SICHERHEIT sprach mit Stefan Dörenbach, Country Manager DACH, über den Ausbau des Teams in Deutschland, Österreich und der Schweiz und die wichtigsten Themen rund um die Videoüberwachung.

◄◄ zurück zum Inhaltsverzeichnis

GIT SICHERHEIT: Das Jahr 2022 war für viele Hersteller in unserer Branche nicht nur wegen der Lieferengpässe eine große Herausforderung. Wie ist Hanwha Techwin durch das letzte Jahr gekommen und wie sind Sie ins neue Jahr gestartet?

Stefan Dörenbach: Das letzte Jahr war natürlich auch für uns herausfordernd, ich denke aber, wir sind stärker aufgestellt als je zuvor. Wir waren immer lieferfähig und konnten unsere Kunden zufriedenstellen. Unsere Lieferzeiten sind zu Beginn des letzten Jahres für ein paar Monate von den üblichen 3-4 Tagen bei begehrten Modellen auf 8-10 Wochen angestiegen. Der Markt ist wirklich global geworden und wenn für ein Projekt in den USA mehrere Hundert Kameras eines Typs für ein Projekt geordert wurden, hatte das globale Auswirkungen. Wir haben aber auch zu den Zeiten der größten Engpässe unsere Kunden gut bedient und bestmöglich unterstützt. Dadurch haben wir selbst im sehr markentreuen DACH-Markt zahlreiche neue Kunden und Projektgeschäft gewonnen. Das zahlt sich jetzt aus, weil wir so die Gelegenheit hatten, neue Kunden von unseren Produkten, ihrer Zuverlässigkeit und Leistungsfähigkeit zu überzeugen. Wir wollen sie natürlich langfristig an uns binden und haben dazu auch das richtige Team. Wir haben das letzte Jahr auch dazu genutzt, uns optimal aufzustellen.



Wie sieht das Team aus und wie ist Hanwha in der DACH-Region strukturiert?

Stefan Dörenbach: In der verschiedenen DACH-Regionen sind wir mittlerweile unter meiner Leitung mit sechs Business Development Manager am Start. Sie kümmern sich um unsere Endkunden bei größeren Projekten z. B. im Bereich Logistik und Retail, und stehen den Systemintegratoren, Errichtern, Ingenieurbüros und Planern zur Verfügung. Darüber hinaus haben wir zwei Kollegen im Pre-Sales, Jens Wittkamp als Inside Sales Manager und Bianca Badeck für das Marketing. Ufuk Yamankilicoglu unterstützt die Kunden als Technical Manager. Durch unser zwölfköpfiges Team können wir unsere Kunden sehr individuell und auf allen Ebenen betreuen. Die Kunden können sich auf uns verlassen und wissen immer, wer ihnen bei uns helfen kann.

Dieses Team steht aber nicht alleine da, sondern wir bekommen starke Unterstützung aus Korea und unserem europäischen Headquarter in Chertsey, UK. Wir treffen uns regelmäßig zu Meetings, um die Strategie zu besprechen, unsere Wünsche zu äußern und über Neuheiten zu sprechen. Hanwha investiert massiv und nachhaltig in die Produkte, ins Personal und ganz speziell in unsere Region. Dadurch können wir unseren Service erweitern, Techniksemiare anbieten und z. B. Planungs- und Ausschreibungsunterlagen in deutscher Sprache zu Vergügung stellen.

Hanwha setzt als Hersteller stark auf KI-Technologie. Was haben Sie hier zu bieten?

Stefan Dörenbach: Sowohl unsere Premium-Produktreihe die P-Serie, als auch die populäre X-Serie sind mit eingebauten KI-Funktionen zur Personen-, Gesichts-, Fahrzeug- und Nummernschilderkennung ausgestattet. Traditionelle Videoanwendungen haben künstliche Intelligenz bislang verwendet, um Fehlalarme zu reduzieren und die forensische Suche in Videos auf Basis von Objektattributen zu ermöglichen. Ganz alltäglich ist mittlerweile auch der Einsatz von KI, die sich auf Metadaten fokussiert. Endanwender suchen heute verstärkt nach aufbereiteten Informationen, die über die einfache Aggregation von Metadaten zu Fahrzeugen, Geschlecht, Alter usw. hinausgehen. Zu diesen weitergehenden Informationen gehören zum Beispiel Statistiken zu Fahrzeugtypen in einem bestimmten Zeitraum oder Aufschlüsselungen des Alters und Geschlechts von Kunden. Durch den unmittelbaren Zugriff auf diese Informationen und das direkte Management erhalten Endanwender tiefere Einblicke und können bessere Geschäftsentscheidungen treffen. Anders ausgedrückt: Informationen werden wertvoller, wenn Anwender ihre Daten auf die jeweils effizienteste und relevanteste Weise nutzen können. Wir können mit Wise Business Intelligence wertvolle Informationen liefern und bieten Lösungen, die genau auf die Bedürfnisse verschiedener Branchen und Einsatzbereiche zugeschnitten sind.

Werfen wir einen Blick in die nahe Zukunft. Was erwarten Sie beim Thema KI im nächsten Schritt?

Stefan Dörenbach: Unsere KI-Technologie wird zukünftig durch sogenannte NPUs (Neural Processing Units) verstärkt. Dabei kommt ein KI-Chip zum Einsatz, der selbstständig lernt und gleichzeitig Video, Audio, Text und Bilder verarbeitet, indem er die Arbeitsweise des menschlichen Gehirns imitiert. In einer Videoanwendung erweitert NPU die KI um Funktionen für Verhaltensanalysen und die Erkennung von ungewöhnlichem Verhalten. Darüber hinaus ist es mit NPUs möglich, KI-Algorithmen direkt nach eigenen Kriterien zu trainieren. In Kürze wird Hanwha Techwin den Wise Detector auf dem Markt einführen, der für die Klassifizierung von Objekttypen trainiert werden kann, die für den Anwender besonders relevant sind. Dazu gehören zum Beispiel Einkaufswagen, Fahrzeugtypen oder auch bestimmte Ereignisse.

Abgesehen von Weiterentwicklungen bei KI, welche Neuentwicklungen dürfen wir von Hanwha erwarten?

Bitte umblättern ▶

◀◀ zurück zum Inhaltsverzeichnis

Stefan Dörenbach: Es kommt sehr viel Neues. Sowohl auf Produktebene, aber auch strategische Neuerungen. Wir arbeiten immer weiter an Produktneuheiten für spezielle Anwendungen wie z. B. den beiden neuen KI-gesteuerten Zweikanal-Multisensor-Kameras, die zwei verschiedene Bereiche mit zwei unterschiedlichen Sichtfeldern überwachen können. Damit sind sie ideal für die Überwachung von Treppen oder Rolltreppen, L-förmigen Korridoren und die Sicherung von zwei benachbarten Bereichen wie z. B. Check-in-Schaltern.

Darüber hinaus kommt in Kürze etwas wirklich Bahnbrechendes, das auf unserer Stärke bei den Kamera-Chips basiert. Bisher sind die Intelligenz und die Möglichkeiten von Kameras auf Softwareanwendungen wie z. B. KI- und Videoanalytikanwendungen beschränkt. Wir arbeiten daran, dass eine Kamera mit einem starken Prozessor gleichzeitig auch als Server arbeitet. Das heißt eine Kamera verwaltet bis zu sechs andere Kameras als Server, speichert bis zu zwei Terabyte an Daten und übernimmt Videomanagementfunktionen. In der Praxis bedeutet das, für manche Anwendungen reicht die Technik in einer Kameras völlig aus, man braucht keinen zusätzlichen Server mit aufgespieltem Videomanagementsystem und kein separates Speichermedium mehr.

Weltweit sind Cloudlösungen stark im Kommen. Wie sieht das in der DACH-Region aus?

Stefan Dörenbach: Es ist in der Tat so, dass mit der zunehmenden Verbreitung von Cloud-basierten Services und der gestiegenen Anzahl an Anbietern, die Anwender Geräte und Systeme heute einfach über einen Cloud-Service integrieren können. Investitionen in zusätzliche Server oder die Netzwerkinfrastruktur sind dann meist nicht erforderlich. Aufgrund bestehender Netzwerke, des Budgets oder der Sicherheitsrichtlinien innerhalb einer Unternehmensgruppe ziehen es aber viele Unternehmen vor, auch weiterhin konventionelle On-Premises-Lösungen mit dedizierten Servern und Software einzusetzen. In diesem Jahr rechnen wir daher auch in der DACH-Region mit einem Wachstum der hybriden Systeme, also der Kombination von On-Premises-Technologie mit der Cloud. Bei On-Premises-Lösungen behalten Anwender dabei die volle Kontrolle vor Ort, während Cloud-Lösungen gleichzeitig ein zuverlässiges Backup kritischer Daten gewährleisten. Wir unterstützen Unternehmen in diesem Bereich mit zwei Lösungen: Wisenet Wave VMS für On-Premises und Wave Sync für cloud-basierten Service. Wave Sync ermöglicht Remote-Zugriff, Remote-Management und Remote-Wartung für sehr viele On-Premises-Systeme.

Ein weiteres, sehr heiß diskutiertes Thema ist die Cybersicherheit. Wie hoch aufgehängt ist das Thema bei Hanwha und wie ist die Situation in der Region?

Stefan Dörenbach: Auf den deutschen Markt hat das Thema nochmal eine höhere Priorität als in vielen anderen Regionen. Das liegt glaube ich daran, dass wir schon als Einzelpersonen sehr großen Wert auf Cybersicherheit legen. Das spiegelt sich auch wieder, wenn man die Entscheider in der Branche fragt. Allen Beteiligten ist das Thema sehr wichtig und durch die technologische Integration mit KI, Cloud und IoT kommen neue Anwendungen und Lösungen hinzu, die ein geschärftes Sicherheitsbewusstsein erfordern. Das wird auch durch eine Studie im Auftrag von Hanwha Techwin bestätigt, die wir in Kürze veröffentlichen werden. Sie zeigt, wie wichtig verantwortungsvolle Videoüberwachung ist und dass Endanwender speziell nach Herstellern suchen, die Cybersicherheit und ethische Technologienutzung in den Mittelpunkt ihres Handelns stellen. Uns als Hanwha Techwin ist die Transparenz bei diesem Thema ganz besonders wichtig und das bedeutet, dass wir selbst kleinste Lücken schliessen, sie sofort kommunizieren und dem Anwender die Möglichkeit geben, sofort die neueste Firmware auf die Systeme zu spielen. Unser spezialisiertes Security Computer Emergency Response Team (S-CERT) führt permanent Tests durch und stellt damit sicher, dass die Lösungen von Hanwha Techwin vollständig vor neuen und gerade erst aufkommenden Bedrohungen geschützt sind. Darüber hinaus hat Hanwha Techwin offizielle Zertifizierungen nach UL CAP, FIPS und TTA erworben, um die Sicherheit seiner Produkte auf höchstem Niveau zu gewährleisten.

Mit welcher Einstellung sollte man dem Thema begegnen?

Stefan Dörenbach: In letzter Zeit hat sich „Zero Trust" als zentraler Trend in der Cybersicherheit etabliert. Im Rahmen des Zero-Trust-Modells müssen alle verbundenen Geräte und Anwendungen im Netzwerk einen Qualifizierungsprozess absolvieren. Dabei gilt, dass es grundsätzlich kein „automatisches Vertrauen" zwischen Geräten und Anwendungen geben darf. Hanwha Techwin plant die kontinuierliche Überprüfung und Weiterentwicklung seiner Lösungen mit Blick auf Zero Trust, um so beispielsweise die Compliance mit dem Security-by-Default-Prinzip sicherzustellen. Die Bedeutung der Cybersicherheit kann insgesamt nicht hoch genug bewertet werden. Erfahrungen aus europaweiten Projekten von Hanwha Techwin belegen, dass die verantwortungsvolle und ethische Technologienutzung zu den zentralen Anliegen von Endanwendern gehört.

Wie positioniert sich Hanwha bei den Videomanagement-Systemen? Setzen Sie auf das eigene System oder mehr auf die Zusammenarbeit mit den großen VMS-Anbietern?

Stefan Dörenbach: Die Entscheidung für unser Wisenet Wave oder für ein unabhängiges Videomanagement-System hängt ganz klar von der Anwendung ab. Hanwha Techwin bietet mit SSM ein VMS der Einstiegsklasse an, und für anspruchsvolle VMS-Projekte auf Unternehmensebene arbeiten wir mit führenden Technologiepartnern zusammen. Wisenet Wave haben wir eingeführt, um den Anforderungen von Projekten im mittleren Bereich gerecht zu werden, wobei der Schwerpunkt auf einer vereinfachten Benutzererfahrung liegt. In komplexen Projekten, wo zum Beispiel an einem Flughafen das Boarding noch getrackt und eingebunden werden muss, also viele externe Systeme eingebunden werden, macht ein VMS mehr Sinn, dass solche integrationen erleichtert. Wir arbeiten deshalb sehr eng mit den VMS-Technologiepartnern wie z. B. Genetec, Milestone oder Qognify zusammen. Unsere Produkte sind dort zum Teil schon vor der Produkteinführung aktiv eingebunden und tief integriert. Das geht weit über eine ONVIF-Integration hinaus. Für kleinere und mittlere Projekte kann ich aber mit meiner langjähriger Erfahrung mit VMS sagen, dass Wisenet Wave wirklich das Maß aller Dinge ist. Für sehr viele Projekte kann ich es nur empfehlen. Das System ist sehr intuitiv zu bedienen, quasi selbsterklärend, ist schnell installiert und bietet einen tollen Leistungsumfang, inklusive einer sehr einfachen und wirkungsvollen Suche. Für die Videoüberwachung gibt es nichts Besseres. ●

Hanwha Techwin Europe
Eschborn
htesecurity@hanwha.com
www.hanwha-security.eu/de

◄◄ zurück zum Inhaltsverzeichnis

Easy. Professional.
SecureWeb.

Behalten Sie Ihre Sicherheits- und Hausautomatisierungssysteme jederzeit unter Kontrolle.

Verwalten Sie alle die Informationen

Zentralen

Lokalisieren Sie die Zentralen auf der Karte

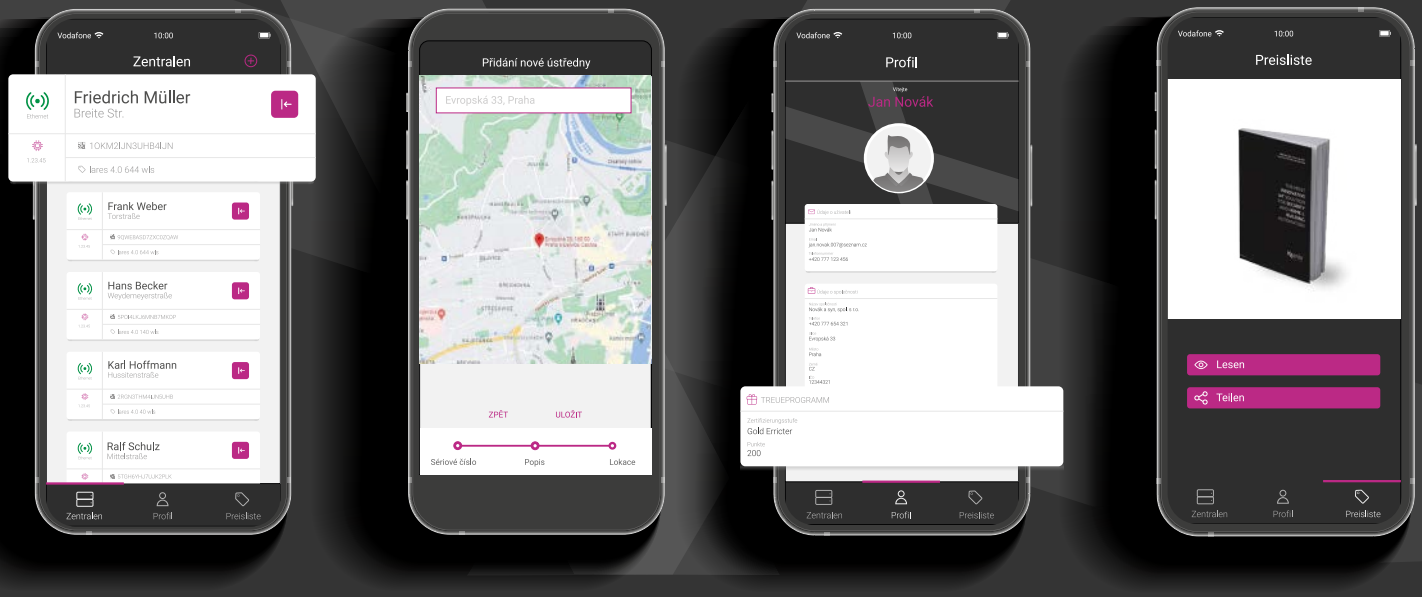
Ort

Individualisieren Sie Ihr Profil und aktualisieren Sie es

Profil

Bleiben Sie mit den neuesten Updates auf dem Laufenden

Preisliste



Easy. Professional. SecureWeb.

Ksenia Security bietet ihren Errichtern einen kostenlosen SecureWeb-Dienst an.

SecureWeb ist eine neue Möglichkeit, um die Systeme zu konfigurieren: Sie können sich direkt mit diesem Portal über PC / MAC oder über die Ksenia Pro App verbinden, die kostenlos aus den Android- oder iOS-Stores heruntergeladen und für jedes Mobile-Gerät verwendet werden kann. So können Sie die Zentrale sogar aus der Ferne programmieren und alle Ihre Installationen von jedem mobilen Gerät, einschließlich Ihres Smartphones, überwachen. Mit der App haben Sie alle Informationen zur Hand: Es ist, als hätten Sie ganze Programmierhandbücher, Preislisten und zahlreiche technische Inhalte in der Tasche, die Ihnen im Bedarfsfall nützlich sein werden.

www.kseniasecurity.com/de

FINDEN SIE MEHR HERAUS

Ksenia®
security innovation

VIDEO

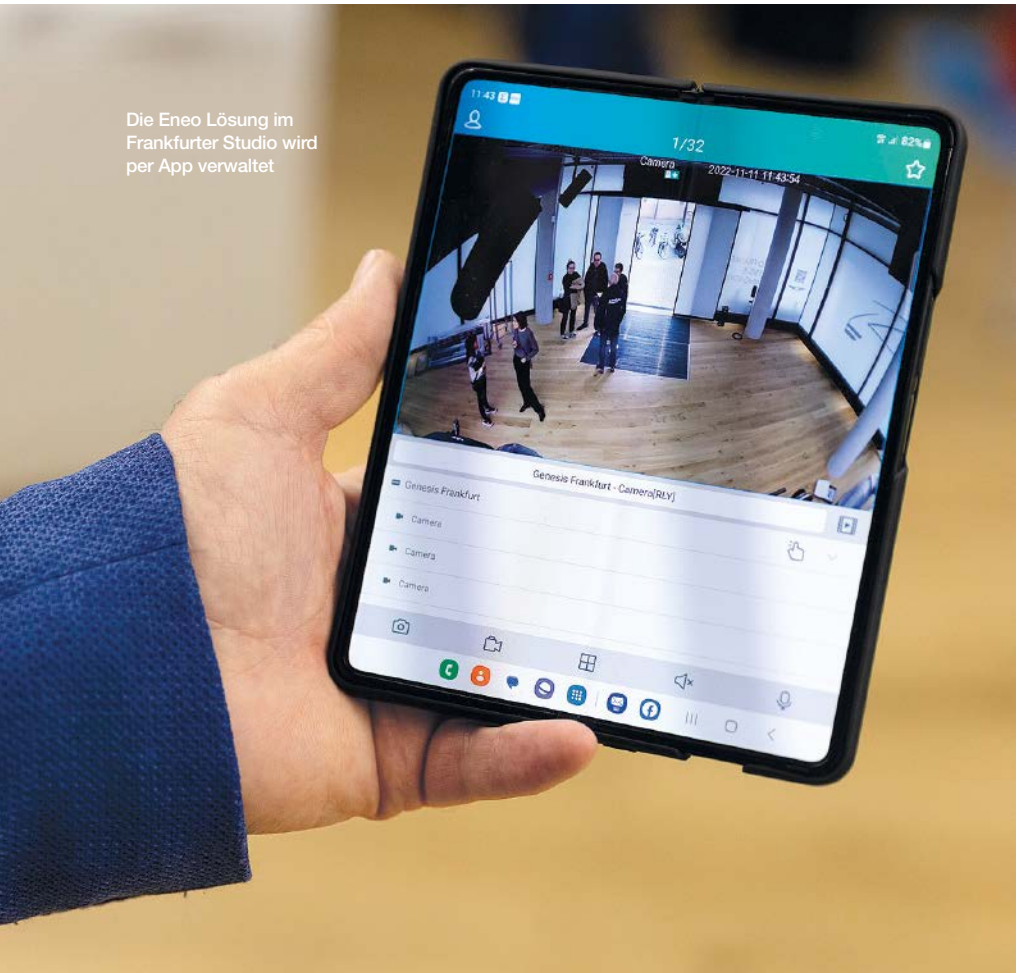
Diskret im Hintergrund

Sicherheit für Luxuslimousinen-Showroom

2021 feierte die südkoreanische Premium-Automarke Genesis ihren Einstand auf dem europäischen Markt. Nach München hat im November 2022 in Frankfurt das zweite Genesis-Studio eröffnet. Für die Sicherheit des exklusiven Showrooms sorgt ein Eneo IN-System, das vom Stuttgarter Systemhaus Mevis.TV in Kooperation mit Digicom Informationstechnologie installiert und in Betrieb genommen wurde.

Form und Inhalt harmonieren bei Genesis auf höchstem Niveau. Das gilt gleichermaßen für die Luxuslimousinen und SUVs der südkoreanischen Premiummarke wie auch für das Kunden- und Serviceerlebnis. Gemäß der koreanischen Tradition, die hierfür den Begriff „son-nim" prägte, sieht man den Kunden nicht so sehr als Autokäufer, sondern vielmehr als Gast, dem die volle Aufmerksamkeit und Wertschätzung entgegengebracht wird – und zwar über den Autokauf hinaus.

Konsequenterweise gibt es bei Genesis keine klassischen Verkäufer, denn die Kundenbetreuung liegt hier in den Händen von Personal Assistants, individuellen Ansprechpartnern, die den Kunden bei allen Fragen rund um ihren Genesis zur Seite stehen – jederzeit, fünf Jahre lang. Steht zum Beispiel ein Service, eine Wartung oder eine Reparatur an, wird das Fahrzeug beim Kunden abgeholt und ein Ersatzwagen bereitgestellt. Wer die besondere Servicementalität von Genesis unverbindlich erleben möchte, kann sich das Modell seiner Wahl auch zur Probefahrt nach Hause bringen lassen.



Die Eneo Lösung im Frankfurter Studio wird per App verwaltet

Diskrete Videosicherheit

Was die Besucherinnen und Besucher des zwischen Hauptwache und Eschenheimer Tor gelegenen Studios dagegen mit Sicherheit nicht bemerken werden, ist das Eneo-System, das im Hintergrund zur Sicherheit der Besucher, Mitarbeiter und ausgestellten Fahrzeuge beiträgt. Für die Installation und Inbetriebnahme zeichnen das Stuttgarter Systemhaus Mevis.TV und die Firma Digicom Informationstechnologie aus Göppingen verantwortlich. Beide Unternehmen blicken auf eine langjährige Kooperation zurück und haben bereits viele anspruchsvolle Projekte realisiert.

Tamer Vural von Digicom führt mehrere Gründe an, weshalb in diesem Projekt die Eneo-Lösung das Rennen machte: „Wir haben unserem Kunden die Eneo IN-Kameras empfohlen, weil sie ideal für diskrete Videosicherheitslösungen sind, vor allem der kompakte Flatdome. Diese Kameras haben den Vorteil, dass sie sehr leistungsfähig sind und kaum auffallen. Und durch die mattschwarze Sonderlackierung, die wir bei Videor in Auftrag gegeben hatten, fügen sie sich organisch in das Studio-Design ein. Ein weiterer Pluspunkt ist die Möglichkeit, das System bequem über Eneo Insight Mobile per Smartphone oder Tablet zu steuern. Wir finden, ein schlankes System, das ohne PC-Client und Monitor auskommt, passt perfekt zum puristischen Design des Studios. Für Eneo und Videor sprachen außerdem die sehr guten Erfahrungen, die wir immer mit dem Vorkonfigurations-Service gemacht haben. Es erleichtert das Arbeiten ungemein, wenn die Festplatten bereits eingebaut und die Kameras eingebunden sind, wenn also geprüfte, montagefertige Systemkomponenten beim Kunden angeliefert werden – ganz besonders natürlich, wenn ein enger Zeitplan einzuhalten ist."

Mehr als bloß Videosicherheit

Insgesamt sind fünf der Kameras im Genesis-Studio Frankfurt im Einsatz. Für den Überblick über die Ausstellungsfläche sorgen vier Flatdomes vom Typ IND-45F0028M0, die hochauflösende, detailreiche Videobilder

Videor Consultant Max Walzer überprüft die Ausrichtung der Kamera mithilfe der Live-Ansicht der App

mit Auflösungen von bis zu fünf Megapixeln liefern. Bildoptimierungsfunktionen wie BLC, HLC, WDR und 3D-DNR sorgen dafür, dass die Kameras auch unter wechselhaften Lichtverhältnissen durchgängig qualitativ hochwertige Bilder aufnehmen. Damit nicht genug, sind die Kameras mit zahlreichen innovativen AI-Videoanalysefunktionen für proaktive Videosicherheitslösungen ausgestattet, die Sicherheitsverantwortliche darin unterstützen können, kritische Situationen möglichst im Entstehen zu erkennen und potentielle Gefährdungen abzuwenden. Hinzu kommen Retail-Intelligence-Funktionen wie Personenzählung, Warteschlangenmanagement und Heat Maps, die wichtige Daten zur Aktivität auf der Verkaufsfläche liefern und so zu einem tieferen Verständnis des Kundenverhaltens beitragen können.

Den hinteren Ausgang des Studios überblickt ein Mini-Dome vom Typ IND-42M2808M0A. Ausgestattet mit einem Sony Starvis CMOS-Sensor und einem motorisierten Varifokalobjektiv generiert diese Kamera Videostreams in Full HD. Das System ist so konfiguriert, dass Anwender jederzeit die KI-basierte Übergangszählung aktivieren können. Gezählt werden dann die Personen, die das Studio über den Haupteingang und den Hinterausgang betreten bzw. verlassen. So wissen die Store-Manager jederzeit, wie viele Personen sich im Studio befinden.

Sascha Kremp (Projektleiter Mevis.TV) und Tamer Vural (Digicom informationstechnologie)

Schlank, leistungsstark, anwenderfreundlich

Die Aufzeichnung und Verwaltung der Videokameras erfolgt mit einem Netzwerkrekorder der Eneo IN-Serie, der mit zwei Festplatten à 4 TB ausgestattet wurde und die AI-Videoanalysefunktionen der Kameras im vollen Umfang unterstützt. Die maximale Auflösung beträgt auf allen IP-Kanälen 8 Megapixel. Anwender können für die Videoansicht diverse Wiedergabemodi wählen, die vom Vollbild bis zum 16-Kanal-Split-Screen reichen. Allerdings erfolgt die Systemverwaltung nicht über den NVR oder einen Client-PC, sondern mittels der App Eneo Insight mobile, die mit wenigen Klicks auf dem Smartphone oder Tablet installiert ist. Die App gibt den Store-Managern rund um die Uhr einen umfassenden Überblick über das Studio, einschließlich Push-Benachrichtigungen im Falle eines Alarmereignisses.

Darüber hinaus unterstützt Eneo Insight mobile Vollbild- und Split-Screen-Ansichten im Live- und Wiedergabemodus sowie Kommunikations- und Interaktionsmöglichkeiten mit Personen im Sichtfeld der Kameras, zum Beispiel per bidirektionaler Audioübertragung oder manueller Aktivierung von akustischen und visuellen Alarmen, sofern diese Funktionen kameraseitig unterstützt werden. Wie bei der Client-Version Eneo Insight haben Anwender auch umfangreiche Möglichkeiten der KI-Ereignisrecherche. Dabei sorgen die zahlreichen Filterfunktionen für ein effizientes und anwenderfreundliches Systemmanagement.

Die Farbe der Kameras wurde an die Umgebung angepasst

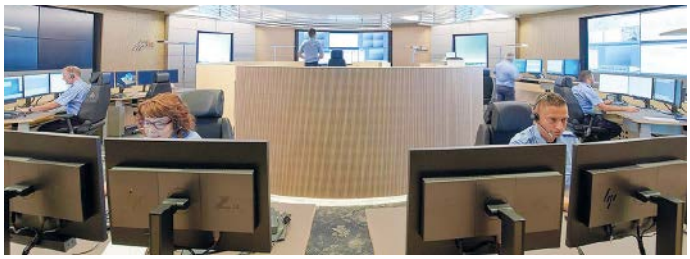
Die Aufzeichnung und Verwaltung der Videokameras erfolgt mit einem Netzwerkrekorder der Eneo IN-Serie mit zwei Festplatten à 4 TB, der die AI-Videoanalysefunktionen der Kameras unterstützt

Geschmeidige Inbetriebnahme

Die Inbetriebnahme erfolgte Mitte November, wenige Tage vor dem Soft Opening des Genesis Studio. Tatkräftig unterstützt durch Videor Consultant Max Walzer, legten Projektleiter Sascha Kremp von Mevis TV und Tamer Vural von Digicom informationstechnologie vor Ort letzte Hand an, ehe sie das System Genesis Studio Manager Carsten Pittelkow und Senior Personal Assistant Guido Becker übergaben. Für gute Stimmung und große Zufriedenheit sorgten neben der schnellen, professionellen Systembereitstellung auch die Performanz und Anwenderfreundlichkeit der Eneo Lösung selbst. Und wenn in Kürze die Genesis Studios Basel und Genf eröffnen, werden auch hier Eneo IN-Lösungen dezent im Hintergrund für Sicherheit sorgen. ●

Videor E. Hartig GmbH
Rödermark
Tel.: 06074 888 0
info@videor.com
www.videor.com

◄◄ zurück zum Inhaltsverzeichnis


© Securiton

Securiton Notruf- und Serviceleitstelle

Integration von intelligenter Videoüberwachung

Videosicherheitssysteme von Securiton überwachen durch intelligente Videoanalyse automatisiert Grundstücksgrenzen und Einrichtungen. Kommt es zu einem Ereignis, werden Live-Daten sofort an die unternehmenseigene Notruf- und Serviceleitstelle übertragen. Und dies sehr detailliert, denn die IPS-Technologie des Unternehmens überträgt mehr als „nur" eine Meldung. Grundsätzlich entscheide der Kunde, welche Detailinformationen weitergegeben werden. Dazu werde gemeinsam festgelegt, welche Szenarien im Meldungsfall ablaufen bzw. welche Interventionsmaßnahmen eingeleitet werden sollen. Und in Folge auch, welche Daten dafür im Detail an die Leitstelle übertragen werden. Sichern beispielsweise Wärmebildkameras die Grundstücksgrenzen ab, werden der Leitstelle im Alarmzeitpunkt nicht nur die Livebilder angezeigt. Zusätzlich bekommt der Leistellenmitarbeiter die Alarmhistorie und den hinterlegten Lageplan im System eingeblendet.

www.securiton.de


© Bosch

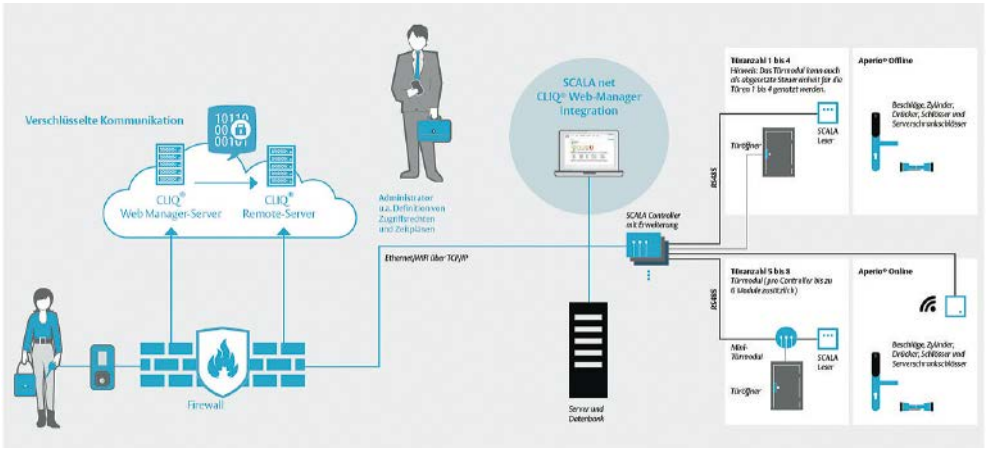
Software-Update

Bosch kündigt eine neue Softwareversion für Praesensa an. Dabei handelt es sich um ein IP-basiertes Beschallungs- und Sprachalarmierungssystem, das hochwertige Audiosignale für Durchsagen oder Musik bietet. Das Software-Update 1.70 für Praesensa bietet ein SIP-Interface für VoIP-Telefonie-Paging und eine Sprechstellen-Sperrfunktion für verbesserte Sicherheit. Die Version kann kostenlos heruntergeladen werden und wird mit einem System-Firmware-Update auf Version 1.70 geliefert. Die Praesensa-Software wurde mit einem SIP-/VoIP-Interface für Live-Sprachtelefonie-Paging erweitert. Es ist nun möglich, eine SIP-Nebenstellennummer mit einer Rufdefinition für Praesensa zu verknüpfen, um Rufpriorität, Vorgong-/Endsignalton und Durchsage-Routing zu konfigurieren. Neben dem Telefonie-Paging dient die SIP-/VoIP-Funktionalität auch als Audio-/Steuerungsinterface für Drittanbietersysteme wie Intercom-, Schwesternruf- und Fahrgastinformationssysteme.

www.boschbuildingtechnologies.com

Whitepaper zu vernetzten Sicherheitslösungen

Ein Whitepaper von Assa Abloy gibt einen Überblick über die Vorzüge der Kombination von eCliq und Scala net. Digitalisierte und vernetzte Sicherheitslösungen bieten bei der Absicherung von Gebäuden und Unternehmen zahlreiche Vorteile. Ein Grund, weshalb der Hersteller die Möglichkeit zur Kombination seiner schlüsselbasierten elektronischen Schließanlage eCliq mit dem kartenbasierten Zutrittskontrollsystem Scala net geschaffen hat. Die Verbindung beider Systeme bietet ein großes Maß an Flexibilität und Nutzerbenefits im gesamten Sicherheitsmanagement einer Gebäudeanlage. Ein aktuelles Whitepaper gibt einen informativen Überblick zu den Vorzügen der Integration beider Schließwelten in einem Verwaltungssystem.



© Assa Abloy

Wer in der Vergangenheit die Vorteile einer schlüsselbasierten elektronischen Schließanlage und eines Zutrittskontrollsystems gleichzeitig in einer Gebäudeanlage nutzen wollte, sah sich mit einem relativ großen Aufwand konfrontiert. Beide Systeme mussten separat und damit auch zwei Datenbanken und zwei Anwendungsoberflächen verwaltet und bedient werden. Dank der neu geschaffenen Scala-Cliq-Schnittstelle ergeben sich für technisch Verantwortliche nun erhebliche Erleichterungen in der Handhabung beider Schließlösungen. Zum einen lassen sie sich komfortabel über eine Benutzeroberfläche verwalten, zum anderen können unterschiedliche Sicherheitsniveaus bei den jeweiligen Nutzergruppen etabliert werden.

Das vorliegende Whitepaper bietet neben einem umfassenden theoretischen Überblick zu den Vorteilen beider Schließsystemlösungen im Einzelnen auch gleich mehrere anschauliche Praxisbeispiele für die gelungene Integration – etwa das einer technischen Hochschule in Deutschland. Dank der Scala-Cliq-Integration erhalten dort Mitarbeiter, die Zugang zu Hochsicherheitsbereichen benötigen, einen elektronischen eCliq-Schlüssel. Andere Mitarbeiter oder Studierende, die sich nur in Gemeinschaftsräumen aufhalten, bekommen wiederum eine Zutrittskarte als Ident-Medium. Die jeweiligen Zutrittsberechtigungen lassen sich von den zuständigen Mitarbeitern bequem über dieselbe Bedienoberfläche in Echtzeit verwalten und bei Bedarf schnell ändern oder löschen, beispielsweise im Falle eines Schlüssel- bzw. Kartenverlusts.

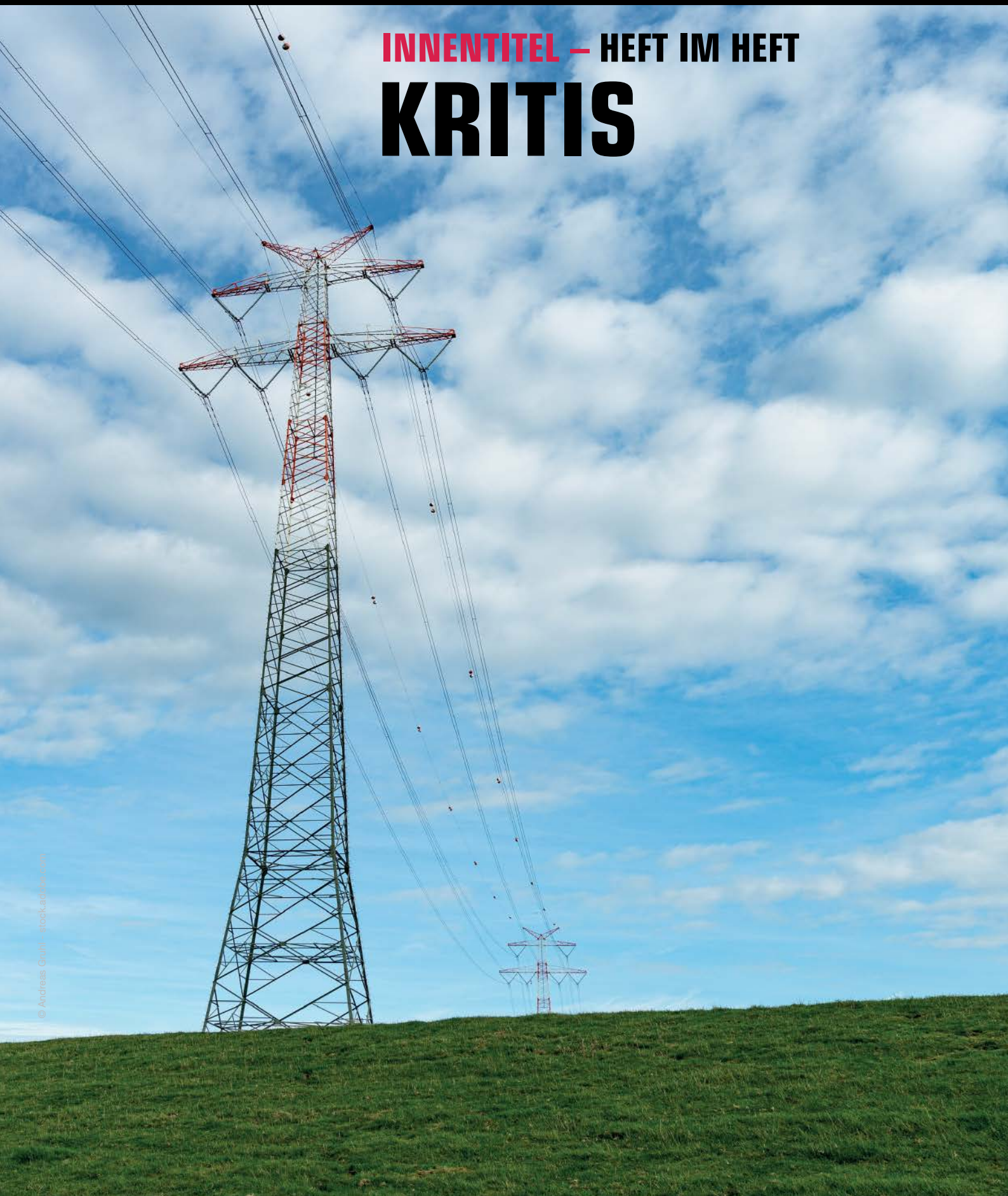
Ein zusätzlicher Vorteil bei diesem Projektbeispiel: Die Zutrittskarte ersetzt den bisherigen Semesterausweis und dient gleichzeitig als Bezahlmedium in der Mensa. Damit bietet die neue Kombinierbarkeit ein hohes Maß an Flexibilität, den Einsatzmöglichkeiten sind jetzt und in Zukunft praktisch keine Grenzen gesetzt. Um mehr über die Lösung zu erfahren, lohnt sich ein Blick in das Whitepaper.

www.assaabloy.com/de

GIT SICHERHEIT

INNENTITEL – HEFT IM HEFT

KRITIS



SICHERHEITSMANAGEMENT

Attacke aufs Eingemachte

Bedrohung und Schutz Kritischer Infrastrukturen

Der prognostizierte Mangel an ausreichender Energieversorgung durch Abbruch der Gaslieferungen aus Russland, der drastische Preisanstieg bei bestimmten Rohstoffen und vor allem die Angriffe auf Nordstream 1 und 2 sowie auf die Kommunikationsnetze der Deutschen Bahn haben die Kritikalität und Bedrohung Kritischer Infrastrukturen (KRITIS) im öffentlichen Bewusstsein, in Politik, Wirtschaft und Medien verstärkt. Die Komplexität der KRITIS, die Strategie, Möglichkeiten und Grenzen für ihren Schutz sowie die Notwendigkeit einer Notfallplanung zu verdeutlichen, ist das Ziel dieses Beitrags von Min. Dir. a. D. Reinhard Rupprecht.

Der Begriff der KRITIS war bis Ende des vorigen Jahrhunderts nicht gebräuchlich. Seither hat er sich aber in der ökonomischen, technologischen und sozialwissenschaftlichen Begriffswelt etabliert. Nach der allgemein anerkannten Definition des Bundesinnenministeriums sind KRITIS Organisationen und Einrichtungen von wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. Die Komplexität der so definierten KRITIS lässt Spielraum für Abgrenzungen. Der Begriff eignet sich hervorragend für politische Bewertungen und strategische Zielsetzungen, bedarf aber als Rechtsbegriff der Präzisierung und der Eingrenzung durch Schwellenwerte.

Die Kritikalität ergibt sich aus der Bedeutung einer Branche, einer Struktur, eines Logistikprozesses, einer Organisation oder eines Unternehmens für den existentiellen Bedarf der Bevölkerung, des Staates oder der Wirtschaft. In seiner Komplexität umfasst der Begriff sowohl KRITIS auf der mikroökonomischen als auch auf der makroökonomischen Ebene einer Branche, einer Volkswirtschaft oder einer internationalen Wirtschaftsgemeinschaft. Nach der aktuellen branchenspezifischen Einteilung des BMI, des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (BBK) und des Bundesamtes für Sicherheit der Informationstechnik (BSI) gehören zu KRITIS die Branchen Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wassernutzung, Finanz- und Versicherungswesen, Staat und Verwaltung sowie Medien und Kultur, nach dem IT-Sicherheitsgesetz 2.0 zusätzlich die Siedlungsabfallentsorgung und „Unternehmen im besonderen öffentlichen Interesse“. Das sind Unternehmen der Rüstungsindustrie, Unternehmen mit IT-Sicherheitsfunktionen für Verschlusssachen, die nach ihrer inländischen Wertschöpfung größten Unternehmen Deutschlands mit Zulieferern sowie Unternehmen, die Gefahrstoffe verarbeiten und unter die Störfall-VO fallen. Insgesamt lassen sich KRITIS mehr als 20 Wirtschaftsbranchen zurechnen.

Gefahren- und Bedrohungsspektrum

KRITIS sind höchst unterschiedlichen Risiken und Bedrohungen ausgesetzt. Sie reichen von dem Mangel an Rohstoffen und Energiequellen über die Vernachlässigung eines Versorgungsbereichs aufgrund politischer oder unternehmerischer Fehlentscheidungen und dem Fehlen qualifizierter Fachkräfte bis hin zu feindlichen, terroristischen, extremistisch motivierten und kriminellen Angriffen sowie katastrophalen Naturereignissen einschließlich Pandemien.

◀◀ zurück zum Inhaltsverzeichnis

Die Breite dieses Bedrohungsspektrums lässt sich durch aktuelle Entwicklungen und Aufsehen erregende Sicherheitsvorfälle verdeutlichen: Die Ausbreitung des Covid19-Virus seit 2020 ist die folgenschwerste Pandemie weltweit seit Menschengedenken, hat Millionen Todesopfer gefordert und das Gesundheitswesen in vielen Ländern überfordert. Auch in Deutschland sind viele Krankenhäuser durch die Vielzahl schwerer Krankheitsverläufe und personelle Engpässe an die Grenzen ihrer Belastbarkeit gestoßen. Die totale Lockdown-Politik in China führt weltweit zu Lieferengpässen und Produktionseinschränkungen. Naturkatastrophen wie die durch einen Tsunami ausgelöste folgenschwere Explosion im Atomkraftwerk Fukushima hat über viele Todesopfer und regionale Zerstörungen hinaus in Deutschland das Ende der Atomindustrie eingeleitet. Die durch den beginnenden Klimawandel verursachten Flächenüberflutungen im asiatisch-pazifischen Raum zerstören die Ernährungsgrundlage für Millionen Menschen.

Der russische Überfall auf die Ukraine im Februar 2022 hat mit der Beendigung des Projekts Nordstream 2 und der Reduzierung der Gaslieferungen aus Russland die Energieversorgung in Deutschland massiv beeinträchtigt. Am 26. September 2022 sprengten unbekannte Täter Lecks in die Gaspipelines Nordstream 1 und 2. Der Anschlag verdeutlicht erneut die Verwundbarkeit der Gasversorgung Deutschlands und anderer europäischer Staaten. Am 8. Oktober 2022 wurden zwei Datenleitungen des Betriebsfunks der Deutschen Bahn in Herne und in Berlin-Karow durchtrennt. Gegen 2 Uhr durchschnitten die Täter zunächst an einer Bahnstrecke bei Herne in einem Kabelschacht, der mit einem massiven Betondeckel gesichert war, mit einer Trennscheibe. Gegen 7 Uhr wurde ein Kabelschacht in Berlin-Karow geöffnet und das Lichtwellenleiterkabel, das als Redundanz für die bei Herne durchschnittenen Kabel diente, durchtrennt. Dadurch fiel das Zugfunknetz GSM-R in Norddeutschland aus. Der gesamte Zugverkehr in Norddeutschland, aber auch internationale Zugverbindungen, waren stundenlang blockiert. Die Täter müssen Hinweise auf den spezifischen Zweck der Datenleitungen gehabt haben.

Ebenfalls im Oktober 2022 sind drei Angriffe auf Internet-Tiefseekabel bekannt geworden. Cyberattacken bedrohen kontinuierlich KRITIS. Zu Beginn des russischen Angriffs auf die Ukraine verloren durch einen offenbar gezielten russischen Hackerangriff auf das Satellitennetzwerk KI-SAT die Betreiber Tausender Windräder in Deutschland die Verbindung zu ihren Anlagen. Ende April 2022 bekannte sich die russische Hackergruppe Killnet zu Attacken auf die Webseiten deutscher Ministerien und Sicherheitsbehörden. Das BSI beobachtet seit Jahren eine zunehmende Entwicklung hin zu aufwendig vorbereiteten ATP (Advanced Persistent Threat)-Angriffen, von denen sich weltweit die Betreiber von KRITIS bedroht sehen. Darüber hinaus bilden die in den letzten Jahren beobachteten Angriffe auf die Software-Lieferketten von IT-Dienstleistern zu ihrer Kundschaft eine neue, besonders beunruhigende Bedrohung.

KRITIS-Strategie

Leitprinzipien der 2009 von der Bundesregierung beschlossenen Nationalen Strategie zum Schutz von KRITIS sind eine enge und vertrauensvolle Kooperation zwischen Staat und Wirtschaft sowie Eignung und Verhältnismäßigkeit staatlicher Maßnahmen zur Erhöhung des Sicherheitsniveaus von KRITIS. Die Strategie fordert dazu auf, Risiken im Vorfeld von Störungen zu erkennen, deren Folgen durch Notfallmanagement und Redundanzen so gering wie möglich zu halten und laufend fortgeschriebene Gefährdungsanalysen sowie Analysen von Störfällen zur Verbesserung der Schutzstandards zu nutzen. Die Nationale KRITIS-Strategie hat der Staat durch Gesetzgebung, Sicherheitskonzepte und Leitfäden umgesetzt. Ziel des IT-Sicherheitsgesetzes 2015 (IT-Sicherheitsgesetz 1.0) war die Erhöhung der Sicherheit informationstechnischer Systeme, insbesondere im KRITIS-Bereich.

Das IT-Sicherheitsgesetz 2.0 aus dem Jahr 2021 erweitert die KRITIS-Regulierung mit mehr Pflichten für KRITIS-Betreiber und mehr Befugnissen für das BSI. Im Koalitionsvertrag 2021 hat die Ampel-Koalition angekündigt, den physischen Schutz Kritischer Infrastrukturen in einem KRITIS-Dachgesetz zu bündeln. Im November 2022 hat die Bundesinnenministerin Eckpunkte für dieses Gesetz vorgestellt. Zum ersten Mal soll das Gesamtsystem zum physischen Schutz Kri-

Dies sollte die Notfallplanung mindestens umfassen

- Festlegung der Verantwortlichkeit im Unternehmen für Notfallplanung und Umsetzung
- Suche nach möglichen Versorgungsalternativen und Beschaffungsvorbereitung
- Beschaffung notwendiger Notstromaggregate für alle Unternehmensbereiche
- Überprüfung der „kritischen Hard- und Softwarekomponenten“, deren Ausfall eine Anlage empfindlich beeinträchtigen würde, nach der KRITIS-VO vom Mai 2021
- Überprüfung der Lieferketten, ihrer Bedeutung und Anfälligkeit sowie der Möglichkeit, Lieferengpässe durch Alternativen und Lagerkapazitäten zu reduzieren
- Vorbereitung des Business Continuity Management
- Vorbereitung personeller Konsequenzen beim Ausfall von Betriebseinschränkungen
- Bildung von Rücklagen für die Beschaffung alternativer Versorgung und den Notfall
- Sensibilisierung der Mitarbeiter für den Notfall und seine Konsequenzen
- Überprüfung und Verstärkung der gesamten Resilienz des Unternehmens
- Planung der internen und externen Kommunikation im Notfall.

© Blue Planet Studio – stock.adobe.com

Bitte umblättern ►

tischer Infrastrukturen gesetzlich geregelt werden. Dazu gehört auch der Schutz vor möglichen Gefahren, die von Herstellern von kritischen Komponenten in KRITIS ausgehen. Auf der Grundlage des Gesetzes sollen wertvolle Erkenntnisse zur Lage in den einzelnen KRITIS-Sektoren in einem umfassenden Lagebild gewonnen werden. Und die Zusammenarbeit der am Schutz Kritischer Infrastrukturen beteiligten Akteure auf staatlicher Seite und bei den Betreibern soll klar strukturiert werden.

Die Resilienz des Gesamtsystems KRITIS wird durch einheitliche Mindestvorgaben für Resilienzmaßnahmen in allen Sektoren gestärkt. Die Auswirkungen auf das Gesamtsystem KRITIS muss beim physischen Schutz Kritischer Infrastrukturen im Vordergrund stehen. Nach einer Pressemitteilung des BMI vom 21. Oktober hat ein Gemeinsamer Koordinierungsstab der Bundesregierung zum Schutz Kritischer Infrastrukturen (GEKKIS) auf Staatssekretärsebene seine Arbeit aufgenommen. Er soll auf politischer Ebene die aktuellen Lagebilder zur Verfügung stellen und einen strukturierten Austausch der Ressorts ermöglichen. Im Rahmen der Nationalen Strategie hat die Bundesregierung schon 2007 einen Leitfaden für Unternehmen und Behörden zum Risiko- und Krisenmanagement für den Schutz von KRITIS erarbeitet und 2011 fortgeschrieben, im Jahr 2014 eine Sicherheitsstrategie für die Güterverkehrs- und Logistikwirtschaft entwickelt sowie ein Rahmenkonzept Notstromversorgung erarbeitet, das vom BBK laufend aktualisiert wird.

Betreiberpflichten

Gemäß § 8b Abs. 3 sind Betreiber von KRITIS verpflichtet, sich beim BSI zu registrieren und eine jederzeit erreichbare Kontaktstelle zu benennen. Nach Abs. 4 haben die Betreiber von KRITIS in dieser Norm definierte Störungen der informationstechnischen Systeme, Komponenten und Prozesse in der im Einzelnen festgelegten Form zu melden. Die KRITIS-Verordnung bestimmt in den §§en 1-7 die Anlagenkategorien und Schwellenwerte zur Abgrenzung in den einzelnen Kategorien und beschreibt in den Anlagen 1-4 Anlagenkategorien und Schwellenwerte in den Sektoren Energie, Wasser, Ernährung, Informationstechnik und Telekommunikation.

Die KRITIS-VO 2021 (Kritis 2.0) senkt einige Schwellenwerte und verschärft Auflagen für die Betreiber. Etabliert wird eine neue Meldepflicht für sogenannte „Kritische Komponenten". Sie müssen vor der Nutzung dem BMI angezeigt werden und dürfen nur mit einer Garantieerklärung der Vertrauenswürdigkeit des Herstellers eingesetzt werden, deren Einhaltung das BSI überwacht. Das BSI wird zu einer nationalen Behörde für Cybersicherheitszertifizierung.

Im September 2022 hat das BSI eine neue Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung (SzA) veröffentlicht. Sie liefert Anhaltspunkte für die Anforderungen an Betreiber von KRITIS sowie prüfende Stellen. Die SzA (Intrusion Detection) basiert auf Algorithmen, die anhand von Log-Dateien Angriffe auf Server oder Netzwerke erkennen. Die Betreiber müssen die Log-Dateien auswerten. Die Bündelung verschiedener Sicherheitssysteme und deren einheitliche Steuerung mit Hilfe von Integrationsplattformen erhöht die Resilienz Kritischer Infrastrukturen. Zu den notwendigen Präventionsmaßnahmen gehört ein detailliertes Business Continuity Planning. Als zentrale Meldestelle hat das BSI die für die Abwehr von Gefahren für die IT-Sicherheit wesentlichen Informationen zu sammeln und auszuwerten, potentielle Auswirkungen auf die Verfügbarkeit von KRITIS zu analysieren, ein entsprechendes Lagebild kontinuierlich zu aktualisieren und unverzüglich die KRITIS-Betreiber über sie betreffende Informationen zu unterrichten.

Mit dem IT-Sicherheitsgesetz 2.0 ändern sich durch die neue KRITIS-VO 2021 auch die KRITIS-Anlagen und Schwellenwerte. Die KRITIS-VO senkt Schwellenwerte bestehender KRITIS-Anlagen, fügt neue Anlagen hinzu und benennt weitere um. Das IT-Sicherheitsgesetz 2.0 legt mehr vorsätzliche oder fahrlässige Verstöße gegen KRITIS-Vorgaben als Ordnungswidrigkeiten fest und definiert deutlich höhere Bußgelder bis zu 2 Millionen Euro, bei Juristischen Personen bis zu 20 Millionen Euro. Das IT-Sicherheitsgesetz 2.0 gilt auch für „Unternehmen im besonderen öffentlichen Interesse". Das sind Unternehmen der Rüstungsindustrie, Unternehmen von besonderer volkswirtschaftlicher Bedeutung und Unternehmen, die der Störfall-VO unterliegen.

Die im November 2022 vom Parlament und Rat der EU angenommene NIS2-Direktive bildet den europäischen Rahmen für IT-Sicherheit der KRITIS-Betreiber. Sie legt Mindeststandards für die Regulierung von KRITIS fest. Spätestens ab Oktober 2024 müssen Unternehmen in 18 Sektoren ab 50 Mitarbeitern und 10 Millionen Euro Umsatz Cybersecurity-Pflichten umsetzen. Die NIS2-Direktive erhöht die kritischen Essential Sektoren auf sieben. Die Sektoren von „important entities" auf 11. Cybersecurity muss nach dieser Direktive auch in Lieferketten betrachtet werden. Mögliche Geldbußen und Enforcement Actions werden deutlich ausgeweitet. Wieviel KRITIS-Betreiber 2021 aufgrund der ersten NIS-Direktive in Cybersicherheit investiert haben, zeigt der „NIS Investments 2022"-Report von ENISA (European Union Agency for Cybersecurity). Danach geben sie nur noch knapp 7 % des IT-Budgets für IT-Sicherheit aus. Ein Drittel aller KRITIS-Betreiber im Energiesektor überwacht keine einzige kritische Betriebstechnik (OT) durch ein Security Operation Center.

Schutz von Strom- und Kommunikationsnetzen

Eine flächendeckende Überwachung der im Erdboden oder auf dem Meeresboden verlaufenden Strom- und Kommunikationskabel ist ausgeschlossen. Allein die Deutsche Telekom hat schon bisher ein Glasfasernetz von mehr als 650.000 km im Boden verlegt. Das deutsche Stromnetz verläuft über 1,8 Millionen km. Ein größerer Stromausfall könnte zum großflächigen Ausfall der Grundversorgung führen.

Auch das Kabelnetz der Deutschen Bahn mit 34.000 km entlang des Schienennetzes kann nicht 100 %ig geschützt werden. Das heißt aber nicht, dass der Betreiber dieses Netzes möglichen extremistisch motivierten Angriffen hilflos ausgeliefert ist. Wichtig ist vor allem die Verlegung redundanter Kabelnetze. Dass die Saboteure in Herne und Berlin wussten, wie sie die Redundanz überwinden konnten, lässt auf Insiderwissen und dessen mangelhafte Geheimhaltung schließen. Wichtig ist auch, dass eine Kabeldurchtrennung mithilfe sensorischer Überwachung lokalisiert und dann schnell behoben werden kann. Im August 2022 veröffentlichte die Bundesnetzagentur ein Strategiepapier zur Resilienz der deutschen Kommunikationsnetze.

Schutz von Versorgungsleitungen

Auch ein 100 %iger Schutz von Versorgungsleitungen im Energiesektor und der Wasserversorgung erscheint unmöglich. Das Erdgas-Fernnetz ist allein auf deutschem Boden über 40.000 km lang. Zwar sind die Stahlröhren überwiegend in 1,5 m Tiefe vergraben. Ein Anschlag wird dadurch aber nicht ausgeschlossen. Der Bundesverband der Energie- und Wasserwirtschaft hält flächendeckende Ausfälle in der Energie- und Wasserversorgung für „sehr unwahrscheinlich. Pipelines auf dem Meeresboden zu schützen ist besonders schwierig. Die Tausende Sensoren, die der Betreiber von Nordstream eingebaut hatte, zeigten die Gefahr erst, als es zu spät war. Umso wichtiger ist es, ein Gasleck rasch detektieren zu können.

Forscher der Chinese Academy of Science haben eine Methode entwickelt, das 3D-Bild einer Leckgaswolke zu erstellen, das detaillierte Informationen über das Leck, dessen Volumen und die Gaskonzentration liefert.

◄◄ zurück zum Inhaltsverzeichnis

Um ein 3D-Bild anzufertigen, nutzen die Forscher zwei Systeme, um 2D-Messungen einer Gaswolke aus verschiedenen Perspektiven zu erhalten. Diese Informationen werden räumlich mit Standortangaben verknüpft. Der neue Ansatz könnte zur Früherkennung, Risikobewertung und Bestimmung der besten Methode zur Behebung des Gaslecks eingesetzt werden.

Schutz von Knotenpunkten und Anlagen

Natürlich lassen sich Knotenpunkte in den Kabelnetzen und Versorgungsleitungen und einzelne KRITIS-Anlagen – etwa Solarparks, Windräder, Überspannwerke, Kraft- und Wasserwerke, Rechenzentren, Krankenhäuser – weit besser als lineare Infrastrukturen mit baulichen Mitteln, mechanischer und elektronischer Sicherheitstechnik vor Angriffen schützen. Solche Anlagen sind andererseits sowohl für Saboteure wie für Cyberkriminelle, die die Steuerungssysteme angreifen, um Daten mit Ransomware zu verschlüsseln und Lösegeld zu erbeuten, leicht erkennbare und attraktive Ziele.

Als Knotenpunkt der Internet- und Telefonverbindungen ist das deutsche Commercial Internet Exchange in Frankfurt am Main bekannt. Knotenpunkte von Tiefseekabeln, die auf Land treffen, werden teilweise rund um die Uhr kontrolliert. Anlagen und Betriebe von KRITIS bedürfen eines doppelten Perimeterschutzes, der aus Ummauerung oder Umzäunung sowie Überwachung durch Videoüberwachung mit Infrarotkameras und intelligenter Bildanalyse sowie im Boden verlegter oder in den Zaun integrierter Detektionskabel besteht. Insbesondere Glasfaser-Überwachungssysteme sind in der Lage, eine zuverlässige, vollautomatische Überwachung des Perimeters zu gewährleisten. Bei Beschädigung des Zaunes kommt es zum Kabelbruch und somit zur Unterbrechung der Signalübertragung. Dadurch wird die EMA aktiviert.

Besonders schutzbedürftige Räume und Anlagen innerhalb von KRITIS, etwa das Rechenzentrum oder zum Beispiel Räume innerhalb eines Krankenhauses, in denen sich besonders wertvolle medizinische Geräte befinden, sind zusätzlich durch Zutrittskontrolle mit Zweifaktor-Authentifizierung zu schützen. Fachleute warnen davor, dass Energieversorgungsanlagen durch das Eindringen in IT-Netzwerke über periphere Infrastrukturelemente angreifbar werden, etwa wenn unbemannte Spannwerke an das Netzwerk angebunden sind. Als Lösungsansatz wird eine Kopplung der Liegenschaftsüberwachung, der betrieblichen Kontrollsysteme und der IT-Sicherheitssysteme durch die Zusammenführung der Daten in einem gemeinsamen Lagebild vorgeschlagen.

Notfallplanung

Zum Schutz von KRITIS gehört jedenfalls auch eine umfassende Notfallplanung für den Fall, dass ein Angriff oder eine sonstige massive Störung oder Zerstörung nicht verhindert werden konnte. Sie basiert auf einer umfassenden, auf die jeweilige KRITIS spezifizierte, Bedrohungs- Gefahren- und Schwachstellenanalyse. Die Notfallplanung muss die Folgen entsprechender Angriffe und Beeinträchtigungen durch andere Einflussfaktoren auf die KRITIS analysieren, mögliche Versorgungsalternativen suchen und vorbereiten. ●

Autor:
Reinhard Rupprecht
Min. Dir. a. D.

VIDEO

Quo vadis, KRITIS?

KRITIS-Dachgesetz, neue Vorschriften und Sicherheitsaspekte

Kritische Infrastrukturen gehören zu den zugleich lebenswichtigen und verletzbaren Sektoren einer Volkswirtschaft. Dies zeigen die jüngsten physischen Sabotageangriffe auf Steuerungskabel der Deutschen Bahn und die Nord-Stream-Pipelines im Herbst 2022. Über aktuelle gesetzliche und regulatorische Entwicklungen – und darüber, wie Betreiber und Hersteller von KRITIS-Komponenten die richtigen Vorkehrungen und informierte Entscheidungen treffen können, – informiert der nachfolgende Beitrag von Jürgen Seiler, Geschäftsführer des zur Dallmeier-Gruppe gehörenden Consultingunternehmens Davidit.

Mit dem Dachgesetz und vertrauenswürdigen Lösungen zur ganzheitlichen KRITIS-Resilienz

Bereits im März 2022 berichtete der „Spiegel" über einen Sonderlagebericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Demnach könnte Deutschland aufgrund der russischen Invasion in der Ukraine schon bald zum Ziel politisch motivierter Cyberangriffe werden. Konkret ging es um sogenannte Hochwertziele, also Schlüsselsektoren der deutschen Industrie. Spätestens seit den Sabotageangriffen auf die Nord-Stream-Pipelines und auf die Steuerungskabel der Deutschen Bahn ist der Schutz von KRITIS stärker in den Fokus gerückt: bei den KRITIS-Betreibern, in der Bevölkerung, aber auch in der Politik.

Jürgen Seiler, Geschäftsführer, Davidit GmbH (Consultingunternehmen der Dallmeier Gruppe)

In der Folge legte das Deutsche Bundeskabinett am 7. Dezember 2022 „Eckpunkte für das KRITIS-Dachgesetz" vor und machte damit deutlich: Bei KRITIS handelt es sich um Industriezweige, die der Staat durch besondere Maßnahmen – klassisch physisch sowie digital cybertechnisch – schützen muss, und durch begleitende Verordnungen und Gesetze absichern und regulieren wird.

„Lex Huawei"

Seit der Verabschiedung des IT-Sicherheitsgesetzes 2.0 im Mai 2021, das als Artikelgesetz unter anderem das BSI-Gesetz geändert hat, gelten für KRITIS-Betreiber neue, verschärfte Sicherheitsanforderungen. Davon betroffen sind auch der neu hinzugekommene KRITIS-Sektor „Siedlungsabfallentsorgung" und die Gruppe „Unternehmen von besonderem öffentlichem Interesse (UBI)". Auch der Kreis und die Anzahl der betroffenen und regulierten Unternehmen wurde durch neue Definitionen und Schwellenwerte erweitert.

Konkret werden mit dem §9b BSIG erstmals auch Hersteller bzw. Vorlieferanten von kritischen Komponenten beim Einsatz in KRITIS in die gesetzliche Pflicht genommen, Stichwort „Prüfung auf Vertrauenswürdigkeit" und „Garantieerklärung". In der Öffentlichkeit ist dies besser bekannt als „Lex Huawei" durch den Aufbau des 5G-Mobilfunknetzes in Deutschland. Der aktuelle Rechtsrahmen für KRITIS ist im BSI-Gesetz, insbesondere in den Paragrafen 8a ff., sowie in der KRITIS-Verordnung 2.0 kodifiziert.

Richtlinie auf EU-Ebene

Nach unserer Einschätzung hat Deutschland mit dem IT-Sicherheitsgesetz 2.0 eine Vorreiterrolle übernommen und ist seinen europäischen Kollegen und deren EU-NIS-2-Richtlinie (Netz- und Informationssicherheit) inhaltlich und zeitlich, wie bereits bei der NIS-1-Richtlinie, zuvorgekommen. Das strenge IT-Sicherheitsgesetz 2.0 dürfte große Teile der neuen NIS-2-Richtlinie bereits umgesetzt haben. Eventuell noch fehlende Teile würden möglicherweise durch das „IT-Sicherheitsgesetz 3.0" und das geplante KRITIS-Dachgesetz in nationales Recht umgesetzt. Dasselbe Umsetzungsszenario gilt auch für die EU RCE-Richtlinie (Resilience of Critical Entities), auch CER-Richtlinie genannt. Das Thema Resilienz spiegelt sich dementsprechend auch im geplanten KRITIS-Dachgesetz wider.

Physische Resilienz fehlt noch

Nach unserer Einschätzung steht hinter dem geplanten KRITIS-Dachgesetz die politische

◄◄ zurück zum Inhaltsverzeichnis

© ON-Photography - stock.adobe.com

Neue Regularien sollen mehr Sicherheit für Kritische Infrastrukturen bringen

© Song_about_summer – stock.adobe.com

Neben staatlichen Stellen bieten auch Hersteller wie Dallmeier hilfreiche KRITIS-Leitfäden an

Erkenntnis, dass für den Schutz und die Resilienz von KRITIS kein „fragmentierter und unkoordinierter", sondern ein ganzheitlicher und hybrider Ansatz verfolgt werden muss. Nur eine Art ganzheitlicher Schutzschirm für KRITIS ist zielführend. Was heißt das konkret? Derzeit gibt es mit dem IT-Sicherheitsgesetz und dem BSI-Gesetz bereits einzelne Regelungen für KRITIS-Betreiber zur Cybersicherheit, aber eben nur zur Cybersicherheit. Auch für die physische Sicherheit gibt es Regelungen, allerdings nur für einzelne KRITIS-Sektoren wie im Luftsicherheitsgesetz. Bundesweite, sektoren- und gefahrenübergreifende „Dachregelungen" zur physischen Sicherung kritischer Infrastrukturen gibt es bisher nicht.

Wir halten die geplanten Regelungen und den Schritt zu mehr physischer Sicherheit aus geopolitischer und sicherheitspolitischer

Ziel: Ganzheitliche Resilienz

Die wichtigsten Eckpunkte für ein KRITIS-Dachgesetz

1. Die Physische Sicherheit soll erstmals gesetzlich reguliert werden

- verpflichtende Umsetzung einheitlicher technischer Mindestschutzstandards
- unter anderem mit Detektionssystemen und Systemen zur Umgebungsüberwachung, zum Beispiel durch Videoüberwachung

2. Definition und Erweiterung der betroffenen KRITIS-Unternehmen

- neuer Sektor (Raumfahrt/Weltraum)
- klare, einheitliche „Wer gehört zu KRITIS"-Definitionen nach qualitativen und quantitativen Kriterien

3. „Vertrauenswürdigkeitsprüfung" von Herstellern

- bei kritischen IT-Komponenten: BSI-Gesetz (§ 9b Abs. 3 BSIG) fordert Garantieerklärungen über Vertrauenswürdigkeit des Herstellers
- bei sonstigen, kritischen Nicht-IT-Komponenten: Für einen umfassenden Schutz werden Regelungen geprüft, um KRITIS vor Einflüssen und Abhängigkeiten von bedenklichen Herstellern aus dem Ausland zu schützen

4. Ganzheitliche Resilienz als Ziel

- physische Sicherheit und Cybersicherheit gemeinsam und übergreifend „denken", überwachen und prüfen („Security Convergence")
- Erhöhung der geopolitischen Resilienz durch obigen optionalen Punkt „Prüfung bedenklicher Hersteller aus dem Ausland"
- Kohärenz beim Cyberschutz und beim physischen Schutz, auch durch enge Zusammenarbeit zweier Aufsichtsbehörden: BSI und BBK (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe)

5. Einbettung in den EU-Rechtsrahmen

- Umsetzung der EU CER-Richtlinie über die Resilienz kritischer Infrastrukturen
- Umsetzung der EU NIS-2-Richtlinie

6. Gesetz und gesetzgeberischer Umsetzungsprozess

- Weiterer geplanter Umsetzungsprozess: im Laufe des Jahres 2023

Bitte umblättern ▶

◀◀ zurück zum Inhaltsverzeichnis

Sicht für begrüßenswert – insbesondere im Hinblick auf die Versorgungsautonomie, Unabhängigkeit und „Business Continuity" der kritischen Infrastrukturen. Darüber hinaus wäre ein solches Dachgesetz auch aus pragmatischen Gründen wünschenswert, wie z. B. rechtsverbindliche Definitionen von KRITIS-Einrichtungen und klare Zuständigkeiten.

Verbot von Videotechnikherstellern im Ausland

Bei Herstellern aus Drittstaaten können nach §9b BSIG Hersteller oder Vorlieferanten kritischer Komponenten in die gesetzliche Pflicht genommen werden. Die USA gehen im Bereich der cyber- und geopolitischen Resilienz noch restriktiver vor: So verbietet das Bundesgesetz NDAA (National Defense Authorization Act) ab 2019 den Einsatz von Produkten zweier großer chinesischer Videotechnikhersteller in Projekten, die die öffentliche Sicherheit, die Sicherheit von Regierungseinrichtungen und die Sicherheit kritischer Infrastrukturen betreffen. Ähnliche Verbotstendenzen sind auch in Großbritannien und anderen Ländern zu beobachten. Auch die Nato und die EU haben im Januar 2023 eine engere Zusammenarbeit beim Schutz von KRITIS vereinbart, insbesondere vor dem Hintergrund geopolitischer Risiken durch autoritäre Akteure.

Videotechnik „Made in Germany"

Wir stellen in letzter Zeit fest, dass der Markt für Videotechnik die Gütesiegel „Made in Europe" und „Made in Germany" zunehmend als Zeichen für Qualität, Sicherheit und Vertrauen wahrnimmt. Errichter und Endkunden fragen verstärkt entsprechende Produkte nach. Es kann daher im Sinne der KRITIS-Gesamtsicherheit nur positiv sein, wenn zu diesem Markttrend „Made in Europe / Made in Germany" auch eine mittelbar steuernde gesetzliche Regelung im BSI-Gesetz oder in einem kommenden KRITIS-Dachgesetz hinzukommt – mittelbar steuernd in Bezug auf vertrauenswürdige Hersteller, Produkte und Komponenten und damit letztlich unmittelbar steuernd zur Stärkung der physischen, cyber- und geopolitischen Resilienz.

Gut beraten mit Handlungsleitfäden

Im Entwurf des KRITIS-Gesetzes vom Dezember 2022 bietet der Staat an, KRITIS-Betreiber mit Handlungsleitfäden zu unterstützen. Zum Thema Videotechnik bietet beispielsweise Dallmeier in seinem kostenlosen Praxisleitfaden „Videotechnologie und Sicherheit für Kritische Infrastrukturen" nützliche Informationen. Erhältlich per Mail: kritis@dallmeier.com ●

Dallmeier electronic GmbH & Co. KG
Regensburg
Tel.: +49 941 8700 0
info@dallmeier.com
www.dallmeier.com
www.panomera.com

Bildanalysefunktionen mit KI

Die Produktlinie „Smart" von Grundig Security umfasst neun Kameramodelle in verschiedenen Gehäuseformen. Die Kameramodelle haben eine Auflösung von 5 bzw. 8 Megapixeln. Ergänzt wird die Produktreihe von vier – teilweise lüfterlosen – Rekordern mit 4, 8 und 16 Kanälen. Ein umfangreiches Zubehörprogramm rundet die NDAA-konforme Produktlinie ab. Die Bildanalysefunktionen werden von künstlicher Intelligenz (KI) unterstützt. Auch kann die Fehlalarmquote bei Einbruchalarm und Perimeterschutz reduziert werden, indem Objekte als „Fahrzeug", „Person" oder „Sonstiges" klassifiziert werden. Die Smart-Kameras erkennen Gesichter in Menschenmengen, zählen Personen und ermitteln die Länge der Warteschlangen an den Kassen eines Supermarkts, damit Ressourcen optimal eingesetzt werden können. Sie informieren, wenn unbefugt Linien überquert oder Bereiche betreten werden, und schlagen Alarm, wenn herrenlose Objekte vor der Tür stehen.

© Abetechs

www.grundig-security.com

Kommunikationsmodul

Mit dem Produkt des Monats im Januar von ABI-Sicherheitssysteme stehen zahlreiche Möglichkeiten offen. Das P-BUS-Kommunikationsmodul KOM zur Anschaltung an die ABI-Systemzentralen MC 1500 über den Peripherie-Bus (P-BUS) ist mit zwei Kommunikationsschnittstellen ausgestattet. Die Kommunikationsschnittstellen können auf folgende Funktionen eingestellt werden: P-BUS-Repeater (2 P-BUS Schnittstellen): Der Repeater bereitet die P-BUS-Daten auf und ermöglicht dadurch die Überbrückung von größeren Distanzen bzw. die Trennung von P-BUS-Segmenten (z. B. bei Mehrbereichsanlagen nach VdS C). P-BUS/M-BUS-Gateway (1 P-BUS und 1 M-BUS Schnittstelle): Das Gateway ist ein Protokollumsetzer und ermöglicht die Anschaltung von M-BUS-Segmenten mit Bus-Meldern und Linienauswertemodulen (LAM) an den P-BUS (z. B. bei Erneuerung von MC 1500-8/-16-Zentralen mit der M-BUS Baugruppe 15341).

© ABI-Sicherheitssysteme

www.abi-sicherheitssysteme.de

Outdoor-Gehäuse Synaps

Mit den Outdoor-Gehäusen Synaps PoE 5 und Synaps PoE 6 von Slat können Kameratypen aller Art angeschlossen werden. Die PoE-Stromversorgung ist für Geräte bis zu 90W mit einer Gesamtleistung von 150W möglich. Alle Kameratypen, wie Dome-, Wärmebild-, Multisensor- und Infrarotkameras sind anschließbar. Der Managed Layer-2-Switch ist mit 5 oder 6 Ports und 1 oder 2 Glasfaserverbindungen ausgestattet. Selbst eine Distanz zum Supervisor bis zu 20 km kann überwunden werden. Mit dem sicheren Webserver mit automatischem First-Level-Support entfallen Wartungseinsätze bei kleineren Problemen. In den Outdoor-Gehäusen finden Kunden Platz, um eigene Geräte wie ihren 4G-Router, ihre Glasfaserkassette, Mikro-PC oder Ähnliches zu integrieren. Die Verwaltung von Datenströmen wird per VLAN, Multicast QoS, SysLog etc. realisiert. So können die Netzwerkleistung und damit auch die Qualität des Bildmaterials optimiert werden.

© Slat

www.slat.com/de

◄◄ zurück zum Inhaltsverzeichnis

© Bilder: Dom

Intelligentes und vernetztes Schließsystem ▲

Dom Sicherheitstechnik kündigt die Einführung von Dom Roq an, eine intelligente Schließlösung, die das Unternehmen in Partnerschaft mit Somfy auf den Markt bringt. Das vernetzte Produkt bietet Sicherheit – und die Gewissheit, sein Zuhause richtig verschlossen zu haben.

Mit Dom Roq schließt der Hersteller die Lücke zwischen mechanischen und digitalen Lösungen. Die Schließlösung ist ausgestattet mit einem mechanischen Zylinder, Einbruchmeldealarm und hochgradig verschlüsselter Ende-zu-Ende-Kommunikation. Dazu kommen die Flexibilität und der Komfort eines smarten Schließsystems mit Benachrichtigungen über den Türstatus, der Möglichkeit, die Tür aus der Ferne mit dem Smartphone zu öffnen, einfacher Freigabe des Zugangs und vielem mehr. Die Schließlösung vereint die vernetzte Motorisierung von Somfy mit Verriegelungs- und Einbruchssensoren, die die Türen der Nutzer ständig überwachen und abnormale Vibrationen sofort erkennen.

Durch die Verbindung dieses Systems mit der Tahoma-Anwendung und ihrem Produktsortiment (Alarmanlagen, motorisierte Zugänge, Garagentore, Rollläden usw.) können die Nutzer die Vorteile ihres vernetzten Zuhauses genießen. Die Deaktivierung des Alarms, die Entriegelung der Haustür und die Öffnung des Tors können kombiniert ausgelöst werden, sobald der Benutzer nach Hause kommt.

Zur Strategie des Herstellers gehört es, smarte Technologie und langjährige Erfahrung in der Haus- und Gebäudesicherheit zu kombinieren. Der Experte für Hochsicherheitszylinder tat sich mit Somfy zusammen. Wie Dom Sicherheitstechnik ist Somfy Mitglied der europäischen SFPI-Gruppe. Somfy ist langjähriger Partner von MAC, der Fenster- und Rolladensparte von SFPI. Dabei ging es Dom vor allem darum, von Somfys Branchenkenntnissen zu profitieren und die Motorisierung von Somfy in die Lösung von Dom zu integrieren. Das Know-how von Somfy in den Bereichen Motorisierung, Elektronik und vernetzte Lösungen mache das Unternehmen zu einem offensichtlichen strategischen Partner, so Alexandre Vigier, Business Anticipation Manager bei Dom Security.

Bei dieser Lösung habe man komplementäres Know-how und Leidenschaft für Technologie in den Dienst von Fachleuten und Endverbrauchern gestellt. Diese Entwicklung mit Dom entspreche voll und ganz dem Ziel von Somfy, der bevorzugte Partner für die Automatisierung von Öffnungen und Schließungen zu Hause und in anderen Gebäuden zu sein, so Florent Ferrer, Direktor der Produktlinie „Secured Access“ bei Somfy. Die Partnerschaft soll auch die Möglichkeit eröffnen, gemeinsam verschiedene Märkte zu adressieren, indem Somfy die Marke Dom in sein Tahoma-System für das vernetzte Zuhause einführt und Dom die Produkte von Somfy auf seinem Fachhandelsmarkt vertreibt.

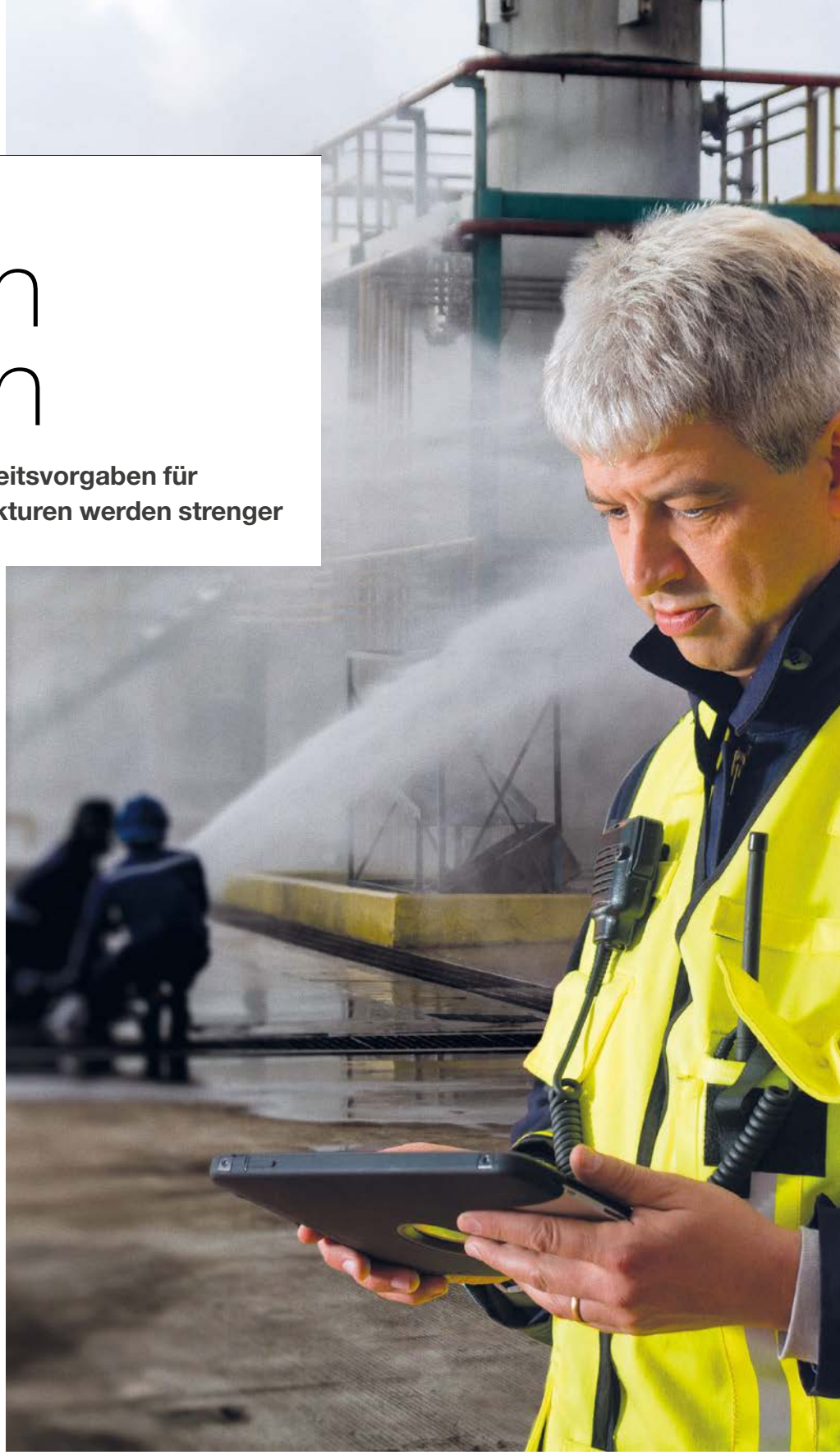
www.dom-security.com

◄◄ zurück zum Inhaltsverzeichnis

KRITIS-DACHGESETZ

Gefahren erkennen

KRITIS-Dachgesetz: Sicherheitsvorgaben für Betreiber kritischer Infrastrukturen werden strenger



Das Bewusstsein für die Sicherheit kritischer Infrastrukturen hat sich erheblich verstärkt – das hängt mit den Auswirkungen der Corona-Pandemie und dem Ukraine-Krieg, aber auch mit anderen Vorfällen in jüngster Zeit zusammen. Ende des letzten Jahres hat die Bundesregierung Eckpunkte für das „KRITIS-Dachgesetz“ beschlossen. Was können Betreiber kritischer Infrastrukturen bereits jetzt tun, um sich darauf vorzubereiten? Ein Beitrag von Johanna Wünsch von Advancis Software & Services.

Mit Beginn der Pandemie im Frühling 2020 wurden sicher geglaubte Lieferketten unterbrochen. Im Bereich der kritischen Infrastruktur waren zunächst insbesondere medizinische Güter betroffen – spätestens mit Beginn des Ukraine-Kriegs jedoch wurde offensichtlich, dass unsere gesamte Versorgungssicherheit nicht mehr durchgängig gewährleistet ist, ob mit Energie, Wasser, Lebensmitteln oder weiteren wichtigen Gütern und Leistungen. Hinzu kamen in den vergangenen Jahren weitere Störszenarien wie z. B. Angriffe auf Gaspipelines, das Ausspähen von Truppenübungsplätzen oder Versorgungsunternehmen mit Drohnen, die Sabotage an Kabeln der Deutschen Bahn oder das Eindringen von Demonstranten in Parlamentsgebäude wie in den USA oder im Irak. Die Anzahl der Sicherheitsvorfälle im KRITIS-Bereich ist gestiegen. Die Reaktion der Bundesregierung darauf war überfällig.

Cyberangriffe und physische Gefahren

Zwar wurden im Bereich der Cybersicherheit vor einigen Jahren bereits mit dem BSI-Gesetz (Bundesamt für Sicherheit in der Informationstechnik) sowie dem IT-Sicherheitsgesetz die Sicherheitsstandards für die kritischen Infrastrukturen verstärkt. Betreiber müssen die Einhaltung ihrer IT-Sicherheitsvorgaben nach dem Stand der Technik regelmäßig gegenüber dem BSI nachweisen sowie erhebliche Störungen ihrer IT melden, sofern sie Auswirkungen auf die Verfügbarkeit kritischer Dienstleistungen haben können.

Darüber hinaus gab es in Deutschland bis jetzt aber kein sektoren- und gefahren-

◀◀ zurück zum Inhaltsverzeichnis

◄ Eine offene Integrationsplattform sorgt für ein umfassendes und effektives Gefahrenmanagement im KRITIS-Umfeld

übergreifendes Gesetz zum KRITIS-Schutz. Allein die Cybersicherheit zu gewährleisten ist jedoch kein umfassendes Konzept. Physische Angriffe wie Sabotage – auch innerhalb eines Unternehmens – oder einfache technische Störungen sowie Naturgefahren können ebenso erheblichen Schaden anrichten.

KRITIS-Dachgesetz

Mit dem KRITIS-Dachgesetz nimmt die Bundesregierung daher nun ergänzend zu den bestehenden Regelungen zum Cyberschutz das Gesamtsystem zum physischen Schutz kritischer Infrastrukturen in den Blick. Das Gesetz soll vor allem einheitliche Mindeststandards festlegen, wie sich Betreiber wichtiger Anlagen schützen und unter welchen Umständen sie Angriffe und Schäden melden müssen. Die Bundesinnenministerin Nancy Faeser erklärte, dass in allen Sektoren der kritischen Infrastruktur „die gleichen Mindestvorgaben im Bereich der physischen Sicherheit“ gelten sollen. Dazu sollen geeignete und verhältnismäßige technische, personelle und organisatorische Maßnahmen getroffen werden.

Was können Betreiber kritischer Infrastruktur bereits jetzt tun, um für diese übergreifenden Sicherheitsvorgaben gerüstet zu sein?

Offene Integrationsplattformen

Natürlich sind KRITIS-Unternehmen bereits umfangreich mit Hilfe technischer Systeme überwacht, doch gerade die Umsetzung übergreifender Aktionen im Gefahrenfall ist oft ein Problem: Was passiert zum Beispiel, wenn es nachts im Maschinenraum eines Heizkraftwerks brennt, während gleichzeitig ein Zaunalarm am rund einen Kilometer entfernten Nebeneingang gemeldet wird, die Sicherheitsleitstelle aber nur mit einem Verantwortlichen besetzt ist?

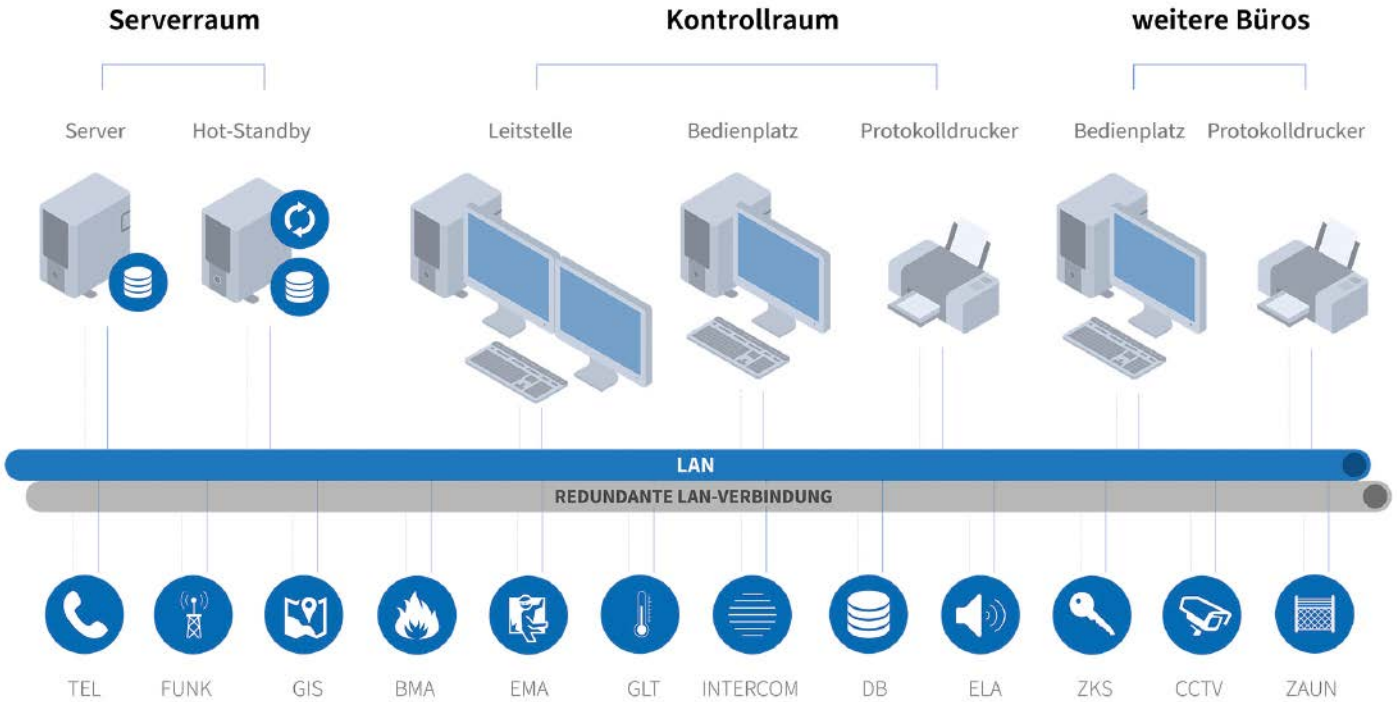
Eine offene Integrationsplattform, die das Gefahrenmanagement sicherstellt – zum Beispiel WinGuard von Advancis – bietet eine zuverlässige Lösung. Statt sich auf viele verschiedene Systeme wie Video- oder Zaunüberwachung, Brandmeldeanlage und Zutrittskontrolle zu konzentrieren, kann das Sicherheitspersonal sich in einer einheitlichen Benutzeroberfläche bewegen und darüber klar erkennen, welche Meldungen kritische Alarme sind. Alle technischen Systeme sind zur einheitlichen Steuerung über Schnittstellen an die Plattform angebunden.

Im Ereignisfall werden eindeutige und individuell auf das jeweilige Unternehmen abgestimmte Verfahrensanweisungen für den Bediener bereitgestellt. Einzelne vorgegebene Handlungsschritte muss er nacheinander abarbeiten, so dass er stets den Überblick behält und die Situation so schnell und sicher wie möglich lösen kann. Gleichzeitig interagieren alle an die Integrationsplattform angebundenen Systeme automatisch.

Systeminteraktion und eindeutige Handlungsanweisungen

Für das Beispiel eines Brandalarms in Verbindung mit einem weiter entfernten Zaunalarm bedeutet dies, dass zunächst über die ebenfalls angeschlossene Videoüberwachung die Kameras im Maschinenraum automatisch in der Benutzeroberfläche aufgeschaltet werden. So kann der Bediener prüfen, ob tatsächlich ein Brand vorliegt und Maßnahmen eingeleitet werden müssen.

Falls ja, bestätigt er dies über die dynamischen Handlungsanweisungen – dann schließen Brandschutztüren automatisch, die Beleuchtung wird eingeschaltet, eine Durchsage zur Evakuierung des Gebäudes wird über die Lautsprecheranlage ausgegeben, die Werkfeuerwehr wird informiert, Feuerwehrlaufkarten werden ausgedruckt usw. Eine direkte Kopplung zu Einsatzleitsystemen ist einfach möglich, wodurch im Notfall ein rasches sowie koordiniertes Eingreifen der Rettungskräfte sichergestellt wird. Hinsichtlich des gleichzeitig eingegangenen Zaunalarms wird der mobile Wachdienst oder der Werkschutz automatisch über eine Meldung auf Mobilgeräte informiert, Schleusen und Tore werden vom System geschlossen. Auch hier wird,



Beispiel-Systemskizze: Alle technischen Systeme sind zur einheitlichen Steuerung über Schnittstellen an die Integrationsplattform angebunden

Bitte umblättern ►

◄◄ zurück zum Inhaltsverzeichnis

falls vorhanden, die Kamera im betreffenden Bereich automatisch aufgeschaltet.

Die Unterscheidung sicherheitskritischer Alarme von Falschalarmen wird durch die Nutzung einer Integrationsplattform erheblich vereinfacht und beschleunigt. Auch Meldungen der Haustechnik oder Wartungsbenachrichtigungen erfolgen über die offene Integrationsplattform, z. B. können Unternehmen mit tausenden von Brandmeldern diese bei Wartungsarbeiten direkt über die Benutzeroberfläche mit Hilfe integrierter CAD-Grundrisspläne einzeln abschalten und nach Abschluss der Arbeiten wieder zuschalten, um Falschalarme zu vermeiden.


© Johanna Wünsch

Johanna Wünsch, Marketing Manager, Advancis Software & Services

Dokumentation und Berichterstattung

Die Dokumentations- und Meldepflicht bei Sicherheitsvorfällen bedeutet für Betreiber kritischer Infrastrukturen oft einen hohen Personal- und Zeitaufwand. Mit einem zentralisierten Gefahrenmanagement über eine offene Integrationsplattform wird die Erfüllung dieser Pflichten erheblich vereinfacht, da für jede Meldung automatisiert ein Bericht erstellt wird. Dieser enthält alle Informationen wie Uhrzeit und Dauer des Alarms, die automatischen Systemmaßnahmen sowie die Aktionen, welche der Bediener durchgeführt hat, usw. Anhänge wie Kamerasequenzen oder zugehörige Pläne werden mitgespeichert.

Der Bericht wird änderungsgeschützt archiviert und kann jederzeit abgerufen und weitergeleitet werden. Die detaillierte Dokumentation unterstützt den Betreiber außerdem bei der weiteren Prozessoptimierung.

Zukunftssicherheit durch technische Erweiterbarkeit

Eine offene Integrationsplattform ist hinsichtlich der Einbindung technischer Systeme flexibel und jederzeit erweiterbar. Auch sehr spezifische, individuelle Schnittstellen und Funktionen sind umsetzbar. WinGuard von Advancis bietet mit der Möglichkeit, dass auch Dritte wie beispielsweise der KRITIS-Betreiber selbst diese entwickeln und einfach in die Software implementieren können, die nötige Flexibilität zur zügigen Umsetzung geänderter Anforderungen in KRITIS-Unternehmen. ●

Advancis Software & Services GmbH
Langen
Tel. +49 6103 80735 0
information@advancis.de
www.advancis.de

Konica Minolta setzt auf Mobotix

Für den Unternehmensschwerpunkt „Sicherstellung der sozialen Sicherheit“ kombiniert Konica Minolta Mobotix-Kameras mit KI-Apps. Das Unternehmen möchte durch seine Geschäftstätigkeit dazu beitragen, Herausforderungen wie das wachsende Risiko von Katastrophen aufgrund des Klimawandels oder das abnehmende Arbeitskräftepotenzial aufgrund alternder Gesellschaften zu lösen. Um die Sicherheit der Menschen zu gewährleisten und die Produktivität der Industrie zu verbessern, wird es immer notwendiger, soziale Probleme durch digitale Transformation (DX) zu lösen, ist Konica Minolta überzeugt. Die KI-unterstützte Echtzeit-Erkennung und -Beurteilung vor Ort unter Verwendung der bildgebenden IoT-Plattform FORXAI von Konica Minolta bietet Lösungsansätze. Konica Minolta setzt dabei auf die robuste, leistungsstarke sowie auf dezentrale Videotechnologie und hohe Cybersicherheit ausgerichtete Mobotix-Videotechnologie.

Die globalen Vertriebsunternehmen von Konica Minolta bieten die Videolösungsdienste auf der Grundlage von Mobotix-Produkten und Dienstleistungen an, um die Arbeitsabläufe bei Kunden zu digitalisieren. Bereits während der Corona-Pandemie in der ersten Hälfte des Geschäftsjahrs 2022 konnte Konica Minolta seine Umsätze in der Videotechnologie mit einer Lösung zum Körperoberflächentemperatur-Screening um 50 % steigern. Daraufhin hat das Unternehmen im April 2022 in Nordamerika begonnen, den Produktvertrieb mit dem von Mobotix zu integrieren. In Europa hat Konica Minolta ab Juni 2022 einen Showroom in Prag eröffnet und Dienstleistungen rund um die Forxai Video Analytic Solution und Forxai Visual Quality Inspection eingeführt. Darüber hinaus begann Konica Minolta im Oktober 2022 mit dem Aufbau einer Serviceeinheit für Videolösungen.

Die im Mai 2022 von Mobotix übernommene Vaxtor Ltd. (Vaxtor) bietet Lösungen zur automatischen Nummernschilderkennung (Automated Licence Plate Recognition, ALPR) und optischen Zeichenerkennung (Optical Character Recognition, OCR). Die Vaxtor OCR-Technologie kann beispielsweise zur Verwaltung, Überwachung und Kontrolle von Lastwagen und Containern in Häfen eingesetzt werden. Sie scannt und erkennt Nummernschilder aus mehr als 150 Ländern und kann Fahrer vor Ort leiten und Zugangsberechtigungen prüfen. Überdies will Konica Minolta durch die Zusammenarbeit mit Mobotix in neue Geschäftsbereiche expandieren, indem es seinen Kunden im Bereich der Verkehrs- und Logistikinfrastruktur mithilfe der KI-Technologie zum Scannen von Nummernschildern und Containern einen größeren Mehrwert bietet.

www.mobotix.com


© Securiton

Alarme und Störungen ▲ zuverlässig im Griff

Als übergreifendes Sicherheitsmanagement hilft SecuriLink UMS von Securiton, kritische Situationen hilfreich zu entschärfen. Das System stellt Informationen sinnvoll bereit und liefert Instruktionen zur Problemlösung. Detaillierte und zoombare Grafiken mit Fotos, Grundrissplänen und Melderpositionen sorgen für eine gute Übersicht. So können auch Mitarbeitende ohne Vorkenntnisse in der Sicherheitstechnik das System problemlos bedienen. SecuriLink UMS informiere übersichtlich, führe die Bediener direkt zu den richtigen Entscheidungen und ermögliche dadurch erfolgreiche Ereignisbewältigung, so Sascha Weis, Produktmanager bei Securiton Deutschland. SecuriLink UMS biete eine intuitiv bedienbare Benutzeroberfläche, die die Informationen auf das Wesentliche reduziert. Das Ergebnis seien schnelle Reaktionszeiten dank definierter Lösungswege, die für jeden Fall individuell hinterlegt sind.

www.securiton.de

Sepura stellt netzwerkunabhängige Tetra-Funkgeräte her

Sepura konstruiert, entwickelt und liefert Lösungen für einsatzkritische und sicherheitsrelevante Anwendungen. Das Unternehmen ist der einzige netzwerkunabhängige Hersteller von Tetra-Funkgeräten, so Hooman Safaie, Regional Director bei Sepura. Es hat eine breite Produktpalette auf Basis des digitalen Tetra- und LTE-Standards. Die Geräte sind mit allen Frequenzen und Infrastrukturen kompatibel. Im Zentrum britischer Hightech-Schmieden in Cambridge beheimatet, ist Sepura ein verlässlicher Partner und Anbieter professioneller Funkgeräte für Nutzer aus den Bereichen öffentliche Sicherheit, Militär, Industrie, Transport, Energie und Gewerbe. Ein starkes Forschungs- und Entwicklungsteam realisiert – in einem eigens errichteten Forschungs- und Entwicklungszentrum in Cambridge – hochmoderne PMR-Produkte und -Lösungen mittels einer Vielzahl von Technologien.

© Sepura

Hooman Safaie, Regional Director bei Sepura: „Sepura ist der einzige netzwerkunabhängige Hersteller von Tetra-Funkgeräten“

www.sepura.com

Zutrittslösungen für Retail- und Filialunternehmen

Salto zeigte auf der EuroShop 2023 in Düsseldorf seine vielseitigen elektronischen Zutrittslösungen. Die elektronischen Zutrittskontrollsysteme kombinieren Sicherheit für einzelne oder mehrere Standorte mit einfacher Bedienung und effizientem Betrieb. Dabei kann jeder Standort seine Nutzer und Türen selbstständig managen. Gleichzeitig sind auch Änderungen aus der Zentrale möglich. Über die Integration mit Drittsystemen lässt sich die Zutrittskontrolle nahtlos in interne Abläufe einbetten und trägt so zur Optimierung von Betriebsabläufen bei. Die Vielseitigkeit der Hardware und Technologien bildet die Basis für individuell abgestimmte Lösungen, die alle Zutrittspunkte wie Türen, Tore, Zufahrten, Aufzüge, Möbel etc. einbinden. Die Lösungen des Herstellers sparen Anwendern Zeit und Geld und gestalten die Wartung effizient, da sie viele tägliche Funktionen und Reaktionen auf Vorfälle automatisieren.

© Salto Systems

Zutrittslösungen von Salto verbessern die Sicherheit

www.saltosystems.de

Produktkatalog von Uhlmann & Zacher erschienen

Der Produktkatalog von Uhlmann & Zacher ist erschienen. Das Unternehmen hat die Produktübersicht inhaltlich und gestalterisch überarbeitet. Der Katalog bietet einen Überblick über das umfangreiche Produktportfolio aus elektronischen Schließzylindern, Türbeschlägen, Möbelschlössern, Wandlesern sowie der notwendigen Infrastruktur, um erfolgreich ein elektronisches Schließsystem zu installieren. Neben der Produktübersicht sind weitere Informationen zu einzelnen Produktausführungen in den dazugehörigen Datenblättern zu finden.

www.UundZ.com

© Uhlmann & Zacher

Produktkatalog von Uhlmann & Zacher

DIENSTLEISTUNGEN

Im Dienst Kritischer Infrastrukturen

KRITIS-Gesetz: Kötter Security fordert stärkere Berücksichtigung privater Sicherheitsdienstleister

Sabotageakte gegen Bahnstrecken und Cyberangriffe auf öffentliche Einrichtungen haben die Sicherheit für Kritische Infrastrukturen (KRITIS) zuletzt wieder verstärkt in den öffentlichen Fokus gerückt. Kötter Security begrüßt vor diesem Hintergrund das jüngst von der Bundesregierung beschlossene Eckpunktepapier für ein Gesetz zum Schutz Kritischer Infrastrukturen. Gleichzeitig mahnt das Familienunternehmen aber eine deutlich stärkere Einbeziehung der privaten Sicherheitswirtschaft bei der Neuausrichtung der KRITIS-Sicherheit an.

Die private Sicherheitswirtschaft ist seit Langem wichtiger Eckpfeiler beim Schutz der Kritischen Infrastruktur, betont Kötter. Die Dienstleister unterstützten seit Jahren Unternehmen der betroffenen Sektoren mit ganzheitlichen Risiko- und Business Continuity Management-Konzepten und übernehmen u. a. durch Sicherheitsdienste und -technik den Schutz von Kraftwerken, Rechenzentren und Internetknoten, (Flug-)Häfen, den Öffentlichen Personenverkehr (ÖPV), Behörden etc.

Die Branche nehme also „eine Schlüsselfunktion“ ein, „die im Eckpunktepapier der Bundesregierung für die geplante Rahmengesetzgebung aber noch nicht ausreichend Berücksichtigung findet“, sagt Dr. Harald Olschok, Mitglied des Kötter-Sicherheitsbeirates. „So werden dort als Ziel zwar u. a. Vorgaben für die physische Sicherheit angeführt; ansonsten bleibt das Papier aber allein auf die staatlichen Behörden und die KRITIS-Betreiber ausgerichtet. Konkrete Ausführungen zu den Dienstleistern, welche die personellen und technischen Schutzmaßnahmen bereits heute umfassend erbringen, fehlen leider gänzlich. Diese Inhalte sollten daher im Rahmen der Gesetzgebung genauso Einzug finden wie die Anerkennung der Sicherheitswirtschaft als eigener KRITIS-

Die private Sicherheitswirtschaft ist ein wichtiger Eckpfeiler beim Schutz der Kritischen Infrastruktur

© Kötter

◄◄ zurück zum Inhaltsverzeichnis

Sektor. Denn die Einstufung als systemrelevanter Sektor ist ein weiterer zentraler Faktor, um ihre Rolle als wichtigen Eckpfeiler der inneren Sicherheit zusätzlich zu stärken."

Solide Sicherheitsarchitektur

Dies unterstreicht auch Wolfgang Bosbach, ebenfalls Mitglied des Kötter-Sicherheitsbeirates: „Ein Eckpunktepapier ist zwar noch kein Gesetzentwurf und ein Gesetzentwurf noch kein Gesetz – dennoch sollte man die Bedeutung solcher Papiere nicht unterschätzen. Die private Sicherheitswirtschaft tritt nicht in Konkurrenz zu den staatlichen Sicherheitsorganen auf, sie will nicht deren Aufgaben in privater Verantwortung übernehmen. Sie ist aber unbestritten ein wichtiger, unverzichtbarer Bestandteil einer soliden Sicherheitsarchitektur. Dies gilt insbesondere für den Bereich der Prävention, denn je wirksamer Gefahrenabwehr funktioniert, desto mehr werden die staatlichen Stellen entlastet. Es wäre nicht nur wünschenswert, sondern unabdingbar notwendig, dass dies auch vom Gesetzgeber erkannt und im Rahmen des anstehenden Gesetzgebungsverfahrens berücksichtigt wird. Sollte das federführende Bundesministerium des Innern und für Heimat dies nicht in eigener Verantwortung berücksichtigen, wäre es Aufgabe des Gesetzgebers hier für eine Korrektur, genauer gesagt: Ergänzung, zu sorgen."

Feste Standards

Kötter-Sicherheitsbeirats-Mitglied Fritz Rudolf Körper hebt die besondere Möglichkeit hervor, die sich aus der von der Bundesregierung geplanten Übernahme der „EU-Richtlinie über die Resilienz kritischer Einrichtungen (Critical Entities Resilience/CER-Richtlinie)" ergibt, die Ende 2022 auf europäischer Ebene verabschiedet wurde und nunmehr innerhalb von 21 Monaten in nationales Recht zu überführen ist. „Diese Regelung ist ein Meilenstein, da erstmals in einer EU-Richtlinie KRITIS-Betreibern verbindlich empfohlen wird, ausschließlich auf Basis fester Standards mit privaten Dienstleistern zusammenzuarbeiten."

Eine Verankerung in der in Folge anzupassenden deutschen Gesetzgebung biete somit die „riesige Chance", das vom Europäischen Dachverband der privaten Sicherheitsdienste (CoESS) seit Langem für Vergaben empfohlene „Bestbieter-Prinzip" sowie dessen hohe Qualitätsstandards für alle Anbieter Kritischer Infrastrukturen in Verbindung mit den hierbei nach Vorgabe der CER-Richtlinie (Art. 16) anzuwendenden Normen verbindlich zu implementieren.

Eine wichtige Orientierung biete hierbei im Sinne der CER-Richtlinie die europäische Normenreihe EN 17483 „Private Sicherheitsdienstleistungen – Schutz kritischer Infrastrukturen", welche mit den grundlegenden Anforderungen im Teil 1 bereits veröffentlicht ist und sukzessive ergänzend sektorspezifische Anforderungen an Sicherheitsdienstleister im KRITIS-Umfeld in den dazu bereits in Erarbeitung befindlichen Normteilen definieren wird. Die Teile 2 und 3 für die Bereiche „Flughafen- und Luftsicherheitsdienstleistungen (Airport and aviation security services)" bzw. „Sicherheitsdienstleistungen für Seeschifffahrt und Seehäfen (Maritime and port security services)" folgen noch in diesem Jahr. ●

Kötter Security
Essen
info@koetter.de
www.koetter.de

KOMMENTAR

Krise und KRITIS-Dachgesetz

Prof. Dr. Clemens Gause, Geschäftsführer beim Verband für Sicherheitstechnik, spricht über die Notwendigkeit der physischen Sicherheit bei Kritischen Infrastrukturen und den Entwurf zum KRITIS-Dachgesetz

Unsere Welt wird immer komplexer und wir stehen ständig neuen und unbekannten Krisen und Katastrophen gegenüber. Damit uns diese nicht unvorbereitet treffen, müssen wir uns entsprechend schützen. Die letzten Krisen haben aufgezeigt, wo unsere Schwachstellen sind und damit auch, wo wir in Zukunft ansetzen müssen. Die Herausforderungen werden vielfältiger, deshalb müssen wir resilienter werden. Das Bundeskabinett hat zu diesem Zweck Eckpunkte des sogenannten KRITIS-Dachgesetzes verabschiedet.

Prof. Dr. Clemens Gause, Geschäftsführer beim Verband für Sicherheitstechnik

Das KRITIS-Dachgesetz ist ein erster großer Schritt, um einem Problem zu begegnen, welches in den letzten Jahren und besonders durch den russischen Angriffskrieg auf die Ukraine immer mehr in den Fokus geraten ist. Bisherige Forderungen des Gesetzgebers richteten sich grundsätzlich in Richtung IT-Sicherheit. Das Härten Kritischer Infrastruktur bezog sich auf Erfordernisse der Informations- und Kommunikationstechnologie. Das umfasst allerdings nur einen Teil der Sicherheit. Wir müssen unsere Kritische Infrastruktur schließlich auch physisch schützen. Neben der IT und der elektronischen Sicherheit ist eben auch die physische oder auch materielle Sicherheit, wie sie im Fachjargon bezeichnet wird, zu beachten. Ansonsten wären beispielsweise Software und Prozesse geschützt, aber der Serverraum und das umgebende Gebäude eben nicht. Ohne physische Sicherheit funktioniert unsere Gesellschaft, so wie wir sie kennen, also nicht.

Das KRITIS-Dachgesetz, welches mit großen Erwartungen und Beifall erwartet wird, hat das Ziel, die Lücken in der physischen Absicherung unserer Kritischen Infrastruktur zu schließen und die Resilienz unserer Gesellschaft in allen Bereichen der KRITIS zu erhöhen.

In den letzten Jahren wurde im Bereich KRITIS viel erreicht: das BSI-Gesetz sowie die BSI-KRITIS-Verordnung haben in den Bereichen Informations- und IT-Sicherheit umfangreiche Schutzmaßahmen und Regelungen auf den Weg gebracht, die die Cyberwelt unserer Kritischen Infrastruktur schützt. Beim Thema physische Sicherheit klafft aber immer noch eine große Lücke. Zwar gibt es zahlreihe Fachgesetze, Standards, Normen und Regelungen, die den physischen Schutz der KRITIS fordern und in verschiedenen Detailgraden beschreiben, aber es fehlt an einem übergreifenden Regelwerk, welches die Befugnisse, Anforderungen und Zuständigkeiten sektor- und gefahrenübergreifend konkret festlegt. An dieser Stelle setzt das neue KRITIS-Dachgesetz jetzt an, es soll, so die Hoffnung, die Regelungen vereinheitlichen und vervollständigen.

Als Voraussetzung für ein solches Gesetz gilt es, die Kritischen Infrastrukturen im Land klar zu identifizieren und abzugrenzen. Das KRITIS-Dachgesetz soll eine Ergänzung und Erweiterung der bisherigen Cybersicherheitsbestimmungen sein und diese nicht ablösen. Vorgesehen sind unter anderem verpflichtende Risikobewertungen, Mindeststandards für Betreiber und ein zentrales Störungsmonitoring. Besonders wichtig bei der Erstellung ist es, sektorübergreifende Regelungen festzulegen, um die Hürden für eine Zusammenarbeit und den fachlichen Austausch zu minimieren. In der jüngsten Vergangenheit haben wir eines gelernt, dass nämlich Krisen Auswirkungen auf mehr als einen Sektor haben. Krisenfolgen in einer vernetzten stark interdependenten Welt bilden unzählige Schnittstellen und Abhängigkeiten heraus. So kann ein Ausfall oder ein sektorspezifisches Problem einen weiteren Sektor betreffen und sich regelrecht durch Systeme hindurchfressen und Folgeschäden, sogar Kaskadeneffekte hervorrufen. In solchen Fällen ist ein schneller Austausch wichtig.

Ich bin froh und dankbar, dass der Verband für Sicherheitstechnik als starke Interessenvertretung der Sicherheitstechnik die aktuellen und zukünftigen Herausforderungen in dieses Gesetz einbringen kann. Der Verband für Sicherheitstechnik vernetzt seit vielen Jahren die Akteure der Sicherheitsbranche und kennt die Anforderungen und Probleme aus erster Hand. Gemeinsam mit Politik, Verwaltung, Wissenschaft und Wirtschaft stellen wir uns regelmäßig neuen Fragestellungen. In unserer Morgenlage, welche wir gemeinsam mit dem Zukunftsforum öffentliche Sicherheit (ZOES), jeden Montag mit Expertinnen und Experten der Branche durchführen, konnten wir wöchentlich neuen Input und Ideen direkt aus der Praxis sammeln und direkt bei den Berichterstattern im Deutschen Bundestag und in der Ministerialverwaltung platzieren. Wir

◄◄ zurück zum Inhaltsverzeichnis

können für unsere Stakeholder mitgestalten und hoffen gemeinsam, ein solides Gesetz auf den Weg zu bringen, welches künftig die Verantwortlichkeiten im Feld der physischen Sicherheit klar regelt, um der zunehmenden Verantwortungsdiffusion entgegenzuwirken. Für physische Sicherheit und Resilienz fühlen sich viele nämlich nicht zuständig.

Bei der Gestaltung eines solchen Gesetzes ist es darüber hinaus besonders wichtig, zukunftsweisende Themen zu betrachten und miteinzubeziehen. Deshalb arbeiten wir seit vielen Jahren in verschiedenen Forschungsprojekten zum Thema Sicherheitstechnik mit, die uns zeigen, was in Zukunft alles möglich sein wird. Dieser Input fließt direkt in die Gestaltung des neuen Gesetzes ein, denn wir können die Probleme von morgen ja nicht mit den Lösungen von gestern bewältigen. Wir müssen neu und unvoreingenommen denken. Unsere Forschungsprojekte bringen genau diese Sichtweise mit ein. Dazu gehören unter anderem der Zufahrtschutz, aber auch Detektion und Umgang mit Drohnen oder beispielsweise das Thema KI in der Sicherheitstechnik. Denn physische Sicherheitssysteme werden zunehmend mit einander und mit anderen Gewerken vernetzt.

Ein spannendes Forschungsprojekt bildet in diesem Zusammenhang SPELL, welches Künstliche Intelligenz in Leitstellen und Lagezentren einbindet. Für das KRITIS-Dachgesetz und das geplante Monitoring stellt SPELL einen Blick in die Zukunft dar, welcher hilft, Resilienz aufzubauen, die uns nicht nur aktuell, sondern auch in den nächsten Jahren in der Bearbeitung von Krisen absichern kann und Prozesse verschlanken und schneller machen kann.

Ich bin gespannt, was die Zukunft in dieser Hinsicht bringt und wie das neue KRITIS-Dachgesetz umgesetzt wird. Es bietet auf jeden Fall viele Chancen und vor allem hilft es uns, Krisen mit Resilienz begegnen zu können und gegen die vielfach konstatierte Katastrophendemenz anzugehen. ●

Informationen zum KRITIS-Dachgesetz:
https://www.bundesregierung.de/breg-de/aktuelles/schutz-kritischer-infrastrukturen-2151164

4K-Displays für Videoüberwachung

Die Serie SMQ für professionelle Videoüberwachung von AG Neovo erkennt jedes Detail in der Dauerüberwachung. Die SMQ-Serie bietet großformatige 4K-Displays. Die Kompatibilität zu BNC-basierten Systemen ermöglicht eine nahtlose Integration der Großbildschirme in bestehende Anlagen. Darüber hinaus bietet sie eine hohe Darstellungsqualität in Verbindung mit digitalen 4K-IP-Kamerasystemen. Die Displays sind mit RS232/LAN-Systemen kompatibel und mit der AG Neovo PID Command & Ctrl-Software steuerbar. Das robuste Design mit Panels und Metallgehäusen gewährt lange Lebensdauer in 24/7-Systemen.

4K-Auflösung mit CCTV-Preset, Auswahl von Gammakurve und Schwarzwertanpassung ermöglichen effektive Optimierung der Bildwiedergabe. Die verbesserte Darstellung insbesondere von nachts oder bei schlechten Lichtverhältnissen aufgenommenen Überwachungsbildern gewährt eine hohe Detail-Sichtbarkeit. Die SMQ-Serie unterstützt BNC-Verkabelung für die Nutzer analoger DVR-Systeme und zeigt dabei Bilder mit einer Auflösung von bis zu 4K für NVR-Benutzer an. Es besteht die Möglichkeit zur Steuerung via RS232- und LAN.

Die SMQ-Serie ist mit einem Panel ausgestattet, das einen 24/7-Dauerbetrieb ermöglicht. Außerdem kommt die Anti-Burn-in-Technologie zum Einsatz, die das Einbrennen des LCD-Panels verhindert und dessen Lebensdauer verlängert. Das äußere Metallgehäuse der SMQ-Serie sorgt für eine Wärmeableitung, um das Kühlsystem zu verbessern und den ordnungsgemäßen Betrieb in kritischen Sicherheitsumgebungen zu gewährleisten.

www.agneovo.com

PERIMETERSCHUTZ

Sensoren, KRITIS und KI

Sensor- und Informationsmanagementsysteme zum Schutz von Infrastrukturen und Einrichtungen

Der umfassende Schutz Kritischer Infrastrukturen insbesondere im Energie- und Versorgungssektor gehört seit Jahren zu den Schwerpunkten von Senstar, einem Anbieter integrierter Sicherheitslösungen einschließlich Videotechnologie, Zutrittskontrolle und Sensoren für den Perimeterschutz. GIT SICHERHEIT sprach mit dem neuen Geschäftsführer Michael Rumpf und Vertriebsleiter John Rosenbusch über die Strategie des Unternehmens für die nächste Zeit – dazu gehören unter anderem die Weiterführung des organischen Wachstums und der weitere Ausbau des Partnernetzwerks.

▲ KRITIS-Sicherungslösungen von Senstar werden z. B. zum Schutz von Öl- und Gasressourcen eingesetzt

© Senstar

Geschäftsführer Michael Rumpf (r.) und DACH-Vertriebsleiter John Rosenbusch – hier im Gespräch mit GIT SICHERHEIT auf der Messe Perimeter Protection in Nürnberg

GIT SICHERHEIT: Herr Rumpf, Herr Rosenbusch, zunächst einmal: Das vergangene Jahr hat ja mit einem traurigen Ereignis geendet: Der Tod von Peter Göring kurz vor seinem geplanten Ruhestand hat nicht nur bei Senstar selbst, sondern in der Branche insgesamt für Betroffenheit gesorgt.

Michael Rumpf: Die traurige Nachricht über den Tod von Herrn Göring hat uns alle im Unternehmen schwer getroffen – sowohl menschlich als auch fachlich. Schließlich war Herr Göring mehr als 20 Jahre lang bei Senstar für die Geschäfte in der Region EMEA verantwortlich, hat maßgeblich den Erfolg und Wachstum des Unternehmens zu verantworten und stand uns als Technischer Leiter der Region immer mit Rat und Tat zur Seite. Das sind in der Tat große Fußstapfen, die es hier auszufüllen gilt.

Herr Rumpf, Sie folgen Herrn Göring ja in der Geschäftsführung nach?

Michael Rumpf: Seit etwa einem Jahr haben wir die strukturellen Änderungen vorbereitet. Seit dem 1. Januar bin ich nun eingetragener Geschäftsführer und Herr Rosenbusch übernimmt jetzt vollständig die Vertriebsleitung in der DACH-Region. Wir sind zuversichtlich, dass Senstar mit diesen organisatorischen Änderungen in der Lage sein wird, seine gesetzten Ziele zu erreichen und mehr Skalierbarkeit zu ermöglichen.

Welche Themen werden für Sie als neuer Geschäftsführer strategisch in der nächsten Zeit im Fokus stehen?

Michael Rumpf: In unserem Fokus steht weiterhin ganz klar das organische Wachstum von Senstar in Deutschland und Europa. Im kommenden Jahr gibt es einige neue Stellen sowohl im Bereich Vertrieb, Business Development aber auch in der Technik zu besetzen. Weiterhin möchten wir unsere Produkte und auch die Aufstellung von Senstar

◄◄ zurück zum Inhaltsverzeichnis

selbst strategisch noch klarer an den von uns gewählten Fokusmärkten ausrichten. Dazu zählen die Umsetzung von Projekten im Bereich der Kritischen Infrastrukturen, Öl und Gas, Justizvollzug und der große Bereich der Logistik. Gerade in diesen Bereichen gilt es unser bestehendes Partnernetzwerk zu pflegen aber auch strategisch zu erweitern. Zusammen mit unserem Mutterkonzern in Kanada werden für diese Bereiche auch immer neue Produkte entwickelt.

Senstar konzentriert sich mit seinen Lösungen auf eine Auswahl vertikaler Märkte. Dabei, Sie erwähnten es gerade schon, spielen Kritische Infrastrukturen, vor allem Anlagen der Energie- und Wasserversorgung, eine besondere Rolle. Geben Sie uns einen Überblick?

John Rosenbusch: Der KRITIS-Bereich ist schon seit einigen Jahren in unserem Fokus. Um die Außengrenzen von Kunden in der Kritischen Infrastruktur zu schützen, haben wir eine große Auswahl an Lösungen, um proaktiv und mit möglichst wenigen Falschalarmen zu alarmieren. Die Nachrüstung unserer Perimeterschutz-Systeme ist unschlagbar einfach zu realisieren und höchst effizient. Die verschiedenen Technologien lassen sich auf alle Projektgrößen skalieren.

In den letzten Jahren haben wir z. B. eine große Anzahl von Solarparks in ganz Europa mit unseren Zaundetektionssystemen ausgestattet, darunter auch der Solarpark Tázlár, der größte Ungarns mit ca. 60 MW Erzeugungsleistung. Unsere Zaun- und Bodendetektionssysteme werden auch verwendet um Umspannwerke, Gasverdichterstationen und unterirdische Gasspeicherkavernen zu sichern. Dazu arbeiten wir eng mit den Strom- und Gasnetzbetreibern zusammen. Aber auch Standorte zur Wasser- und Abwasseraufbereitung bis hin zu Kernkraftwerken werden mit Senstar-Systemen geschützt.

Bevor wir über konkrete Lösungen sprechen – lassen Sie uns erst noch mal Ihr Sortiment etwas aufschlüsseln: Sie sagen ja, dass Sie das größte Portfolio an Produkten der Sicherheitsindustrie vorhalten – wie genau verhält es sich damit?

John Rosenbusch: In der Tat hat Senstar vermutlich die größte Palette an Detektionssystemen am Sicherheitsmarkt zu bieten. Angefangen von verschiedenen Zaundetektionssystemen über Mikrowellenstrecken zur Freilandsicherung bis hin zu Bodendetektionssystemen ist alles dabei. Die Systeme verfügen über eine präzise Signalauswertung, mit denen man metergenau Eindringlinge erkennen kann. Ein Highlight dabei sind sicher die faseroptischen Erkennungssysteme, mit denen man bis zu 80 km Zaun mit einem einzigen System zuverlässig absichern kann. Diese werden auch für die Leckerkennung an Pipelines oder den Schutz von Leitungsnetzen im Kommunikationsbereich eingesetzt. Obendrein gibt es noch unsere Symphony Common Operating Plattform, die Videomanagement, KI-gestützte Videoanalyse, Zutrittskontrolle, Business Intelligence und natürlich unsere Sensoren, benutzerfreundlich vereint. Entwicklung und Produktion aller Produkte erfolgt ausschließlich in Kanada und den USA. Wir unterstützen unsere Kunden auch bei Komplettlösungen und Planungen der Systeme.

Kennzeichnend für Senstar ist insbesondere die Verbindung mit dem Thema Videoanalyse. Sie haben dafür ja vor Jahren schon den Spezialisten Aimetis erworben...

Michael Rumpf: Herr Rosenbusch und ich haben beide früher für Aimetis gearbeitet und ein starkes Partnernetzwerk im Bereich VMS und Videoanalyse aufgebaut. Die Verschmelzung der beiden kanadischen Unternehmen Aimetis und Senstar, beide mit ähnlicher Philosophie, war strategisch eine sehr gute Entscheidung. Das Sortiment beider Firmen ergänzte sich perfekt und ließ uns in den letzten Jahren eine sehr fruchtbare Synergie entwickeln. Gerade unsere langjährigen Partner konnten daraus profitieren, denn mit dem Erfahrungsschatz beider Firmen ist uns es möglich hybride Systemdesigns zu entwickeln, die verschiedene Detektionssysteme und Videomanagement einschließlich Videoanalyse nahtlos miteinander integrieren. Solche Systeme sind hoch effizient und kostengünstiger als reine Videolösungen.

Daraus ist eine Senstar-Spezialität geworden, die Sie als Sensorfusions- bzw. Hybridkonzept bezeichnen – das heißt unter anderem, dass Sie die jeweiligen positiven Eigenschaften von Videoanalyse- und Zaundetektionssystemen miteinander kombinieren und die jeweiligen Nachteile ausschalten. Wie sieht das genau aus?

John Rosenbusch: Sensor-Fusion ist die konsequente Weiterentwicklung solcher Hybridkonzepte. Die Metadaten der Video- und Zaunanalyse werden dabei über eine KI zusammengeführt, mit dem Ziel die Falschalarmrate auf nahezu null zu reduzieren. Die Sensor Fusion-Engine ist mehr als nur eine einfache Boolesche Logikintegration: Sie greift auf Low-Level-Daten zu, um potenzielle Risiken intelligent zu charakterisieren. Durch die Datensynthese kann das System ein Leistungsniveau erreichen, das über dem der einzelnen Sensoren liegt.

Für Sicherheitsanwendungen hat dies unmittelbare, praktische Vorteile, näm-

Bitte umblättern ▶

© hramovnick – stock.adobe.com

Stromversorgungsanlagen sind ständig dem Risiko von Angriffen, Vandalismus und Diebstahl ausgesetzt

© Senstar/Alexey Achepovsky

Senstar-Videomanagement-Lösung Symphony im Kontrollraum

© adempercem – stock.adobe.com

lich die Möglichkeit, die Stärken einzelner Sensortechnologien zu maximieren und gleichzeitig ihre Schwächen zu vermeiden. Wenn die Signalreaktionsdaten der Außensensoren mit den Videoanalysedaten synthetisiert werden, werden störende Alarme, die durch Wind oder Schatten verursacht werden, praktisch eliminiert, während die hohe Erkennungswahrscheinlichkeit des Systems erhalten bleibt. Uns ist es gelungen, damit ein neuartiges Produkt zu schaffen, dass es so auf dem Sicherheitsmarkt sicher noch nicht gibt.

Vergleichen wir also einmal den Perimeterschutz, sagen wir, eines Logistikgeländes mit Lagern und ähnlichem mit denen eines Gaskraftwerks oder Umspannwerks: Ein wesentlicher Hintergrund für jede Sicherheitstechnik ist hier ja die Gewährleistung von Ausfallsicherheit. Das bedeutet vermutlich, dass Sie hier das Maximum dessen einsetzen können, was Ihr Portfolio hergibt...?

Michael Rumpf: Hier gibt es nicht wirkliche Unterschiede. Der Schutzbedarf im Logistikbereich ist ähnlich hoch. In Logistikhallen und Umschlaglagern befinden sich mitunter enorme Warenwerte, gefährliche Güter und Fahrzeuge, die es gegen Diebstahl oder Manipulation zu schützen gilt. Im KRITIS-Bereich möchte man Anlagen aus ähnlichen Gründen schützen und Eindringlinge natürlich auch so früh wie möglich und zuverlässig erkennen. Deshalb greift man häufig auf redundante Systemkonzepte zurück. Meist wird hier also eine Kombination aus Zaun- und Bodendetektion eingesetzt und diese Systeme natürlich mit Videokameras unterstützt.

Wasserversorgung: Aufbereitungsanlagen, Pumpstationen, Speichertanks und Reservoirs müssen gesichert und überwacht werden

Gerade was Projekte im Bereich Kritische Infrastrukturen angeht, arbeiten wir auch eng mit den Herstellern von Zaunsystemen zusammen. Zum Beispiel haben wir erst letztlich für einen deutschen Energienetzbetreiber ein Systemkonzept entwickelt, bei dem ein spezieller Stabgitterzaun entworfen wurde, der einen Durchbruch bzw. Überstieg erheblich erschwert. Die Zaunelemente wurden so gestaltet, dass eine verdeckte Kabelführung u. a. unseres Sensorkabels möglich ist. Somit können wir Ereignisse am Zaun zuverlässig erkennen und das Detektionssystem ist speziell geschützt.

Auch Schnittstellen zu anderen Sicherheitssystemen sind natürlich häufig ein Thema – und auch die Aufschaltung der Meldungen an externe Wachdienste, da die zu schützenden Anlagen häufig etwas ab vom Schuss liegen.

Könnten Sie einmal das eine oder andere typische Projekt skizzieren?

John Rosenbusch: Bleiben wir doch vielleicht beim Klassiker – dem Solarpark. Diese werden üblicherweise mit Maschendraht- oder Stabgitterzäunen umfriedet. Kleine Anlagen haben einen Umfang von 2 bis 3 km, große Anlagen auch gerne mal 20 km, die in einzelne Felder unterteilt sind. Um zu erkennen, ob ein Eindringling über einen Zaun klettert, diesen durchtrennt oder durchbricht, setzen unsere Partner gern das Zaundetektionssystem FlexZone ein – ein sehr zuverlässiges und einfach zu installierendes System, was obendrein auch noch kostengünstig ist und damit perfekt für die Budgets in Solarparks. Das System wird am Zaun montiert, Tore im Zaunverlauf überwachen wir mit drahtlosen solarbetriebenen Meldern. FlexZone erkennt einen Eindringling auf ein Zaunfeld genau und meldet das Ereignis per Schaltkontakt oder Softwareschnittstelle an ein übergeordnetes Videosystem. Dieses steuert automatisch eine PTZ-Kamera auf die entsprechende Alarmzone am Zaun und schon hat das Sicherheitspersonal alle nötigen Informationen um zu sehen, was wo auf dem Gelände vor sich geht. Das Meldesystem am Zaun kommt mit wenig elektrischer Leistung aus und lässt sich deshalb auch problemlos über lange Zeit Notstromversorgen lässt.

...haben Sie noch ein Beispiel parat...?

John Rosenbusch: Ein anders spannendes Beispiel wäre der Schutz von Leitungs- und Kommunikationsnetzen. Pipelines oder auch Kabelwege zur Datenkommunikation werden oft über sehr lange Strecken unterirdisch verlegt. Aber auch solche Medien müssen gegen Sabotage oder Zerstörung durch Schachtarbeiten geschützt werden. Mit einem unserer FiberPatrol-Systeme können wir bis zu 100 km dieser Medien überwachen. Das System unterscheidet maschinelle Schachtarbeiten in bis zu 30 m Entfernung, schwere Fahrzeugbewegungen oder Personenbewegungen von den üblichen Hintergrundvibrationen im Boden und meldet einen Alarm inkl. der zugehörigen GPS-Koordinaten, wenn die Erkennungskriterien erfüllt sind. So können Schäden oder Eingriffe am Leitungsnetz schnell und zuverlässig erkennt und verhindert werden.

Zur Realisierung all dessen pflegen Sie eine Reihe von (Technologie-)Partnerschaften. Geben Sie uns einen Überblick?

Michael Rumpf: Wenn verschiedene technische Sicherheitssysteme zusammenarbeiten sollen, muss das zuverlässig, störungsfrei und vor allem über einen möglichst langen Zeitraum funktionieren. Dazu arbeiten wir eng mit Partnern der Branche zusammen, und schaffen Schnittstellen zwischen unseren Systemen. Ein gutes Beispiel ist die Firma Advancis, die sowohl Schnittstellen unserer Detektionssysteme aber auch unserer Videomanagementsysteme in Ihre Winguard-Lösung anbietet. Natürlich gibt es viele Partnerschaften mit Anbietern von Netzwerkkameras, wie z. B. Axis, Bosch oder Hanwha. Wettbewerb hin oder her, auch mit Firmen wie Genetec oder Milestone führen wir Technologiepartnerschaften, um die Meldungen unserer PIDS-Systeme auch in deren Managementsoftware zugänglich zu machen. Eine sehr frische Partnerschaft haben wir z. B. mit der Firma Wasabi Technologies geschlossen. Dadurch ist es unseren VMS-Kunden möglich, Videodaten datenschutzkonform auch in der Cloud zu speichern.

Herr Rosenbusch, Herr Rumpf, nach einem in vieler Hinsicht ereignisreichen Jahr 2022: Was wird Senstar im neuen Jahr schwerpunktmäßig beschäftigen?

Michael Rumpf: Wir werden uns, wie schon in den vergangenen Jahren, als Firma und produktseitig an den wirtschaftlichen Gegebenheiten sowie an die Sicherheitslage anpassen müssen. Auch wenn die allgemeine Verfügbarkeit von technischen Bauteilen besser zu werden scheint, bleibt es nach wir vor ein spannendes Thema, was uns viel Arbeit und gute Planung abverlangt, um unsere Kunden auch weiterhin verzögerungsfrei beliefern zu können. Ansonsten gibt es natürlich eine Vielzahl an Projekten abzuarbeiten und die richtigen Leute für unser organisches Wachstum zu finden. Das Jahr bleibt spannend, da es gerade im Bereich Videoanalyse und KI viele neue Themen geben wird, und auf diese Reise wollen wir unsere Partner und Endkunden mitnehmen. ●

Senstar GmbH
Maintal
Tel.: +49 6181 5704 100
senstar-gmbh@senstar.com
www.senstar.com

◀◀ zurück zum Inhaltsverzeichnis

Drohnendetektionssystem Aartos

Das Anti-Drohnen-System Aartos der Aaronia AG stand auf der Perimeter Protection im Mittelpunkt. Die Sonderfläche „U.T.SEC – Platform for Drones, Unmanned Technologies and Security“ war erstmalig in die Messe integriert worden.

Wenn es um Perimeterschutz geht, spielt Drohnendetektion und -abwehr in vielen Fällen mittlerweile eine zentrale Rolle. Sei es zum Schutz von Firmengeländen oder Ausbildungsplätzen des Militärs vor Spionage oder zur Sicherung von Kritischen Infrastrukturen im Versorgungs- oder Verkehrssektor, vor Vandalismus oder terroristischen Angriffen. Der Schutz vor versehentlich oder absichtlich illegal eingesetzten Drohnen ist für Sicherheitsexperten und -beauftragte inzwischen integraler Bestandteil moderner Sicherheitskonzepte. Damit einher geht, dass für den Einsatz von Drohnen genauso wie für ihre Detektion und Abwehr politische Rahmenbedingungen unerlässlich sind. So machte sich u. a. der bayrische Innenminister Joachim Herrmann ein Bild von den Möglichkeiten modernster Drohnendetektion und -abwehr auf dem Stand der Aaronia AG.

Aartos bietet einige zentrale Alleinstellungsmerkmale. So bestimmt das System nicht nur die Position und Geschwindigkeit von Drohnen, sondern auch deren Höhe. Es gewährleistet die Highspeed-Ortung von Drohnenaktivitäten. Dafür scannt es das gesamte Frequenzspektrum, inklusive gleichzeitiger Scans unterschiedlicher Frequenzen, und ermöglicht so das Auffinden aller, nicht nur handelsüblicher Drohnen. Die Positionsbestimmung nicht nur der Drohne, sondern auch ihres Operators ermöglicht Aartos in Echtzeit. Ein entscheidender Vorteil, wenn es um die schnelle, erfolgreiche und gesetzkonforme Abwehr von Gefahrenlagen geht. Dabei spielt die Aaronia-eigene Softwarelösung RTSA-Suite Pro eine entscheidende Rolle. Denn die mächtige Echtzeit-Spektrumanalyse-Software ermöglicht die Einbindung verschiedenster Hardwarekomponenten zur Auswertung und gewährleistet somit eine einfache, effiziente und optimale Nutzung des jeweiligen Systems.

© Wiley/GIT SICHERHEIT

Aaronia-CEO Thorsten Chmielus zeigt GIT SICHERHEIT das Aartos-System

Wie maßgeschneiderte Lösungen für die unterschiedlichsten Bedarfe aussehen können, zeigte der Hersteller mehr als 400 Sicherheitsexperten in Fachberatungen und mit einer Vielzahl von Demos zu den Einsatzmöglichkeiten der verschiedenen Aartos-Systeme auf dem Messestand. Vom Aartos DDS X2, das sich beispielsweise zum Schutz von JVAs eignet, bis zum Aartos DDS X9 Pro, das u. a. zum Schutz von Flughäfen genutzt wird, zeigte der Hersteller die ganze Bandbreite seiner Lösungen.

„Das große Interesse des Fachpublikums an unseren Lösungen zeigt uns zum einen den zunehmenden Bedarf in allen sicherheitsrelevanten Sektoren. Zum anderen bestätigt es, dass wir mit unseren modularen Lösungen in der Lage sind, die unterschiedlichsten Bedarfe optimal zu bedienen“, so Thorsten Chmielus, CEO und Gründer der Aaronia AG.

www.aaronia.de

Das System ViPRO.gms ist für den Einsatz in Sicherheitszentralen und -leitstellen konzipiert

BESCHALLUNGSSYSTEME

Gibt Laut, bevor es kritisch wird

KRITIS: Menschenleben und Sachwerte frühzeitig schützen

Sicherheitsrelevante Systeme sind komplex und müssen gleichzeitig der Anforderung höchstmöglicher Verfügbarkeit genügen. An dieser Stelle setzt das Gefahrenmanagementsystem von Funkwerk an: ViPRO.gms reagiert nicht nur auf tatsächliche Fehlermeldungen, sondern unterstützt den Anwender auch dabei, auf mögliche Probleme in den Systemen aufmerksam zu werden, bevor es zum Störfall kommt. Die Software führt alle sicherheitsrelevanten Systeme in einer Oberfläche zentral zusammen und ist als eine der ersten Lösungen dazu in der Lage, das Beschallungssystem von Funkwerk vollständig über IP-Strukturen einzubinden.

Mit ViPRO.gms stellt Funkwerk eine Gefahrenmanagementlösung mit einem vollständig via IP-Strukturen eingebundenem Beschallungssystem vor. Das dabei verwendete Beschallungssystem Cura – ebenfalls aus dem Portfolio des Herstellers – ist ein kompaktes und skalierbares IP-Beschallungssystem, das die Funktionen eines Ansagegerätes und einer Beschallungsanlage in einem Gerät vereint. Zusätzlich bietet Cura viele Überwachungseigenschaften. Es überwacht u. a. Hard- und Softwarekomponenten sowie angeschlossene Lautsprecherlinien auf Erdschluss, Kurzschluss und Unterbrechung. Fällt eine angeschlossene Lautsprecherlinie oder ein einzelner Lautsprecher aus, erzeugt das System eine Warnung, die dem Anwender über das System ViPRO.gms ausgespielt wird.

In Bereichen der Kritischen Infrastruktur, wie z. B. einem Kraftwerk, stellt das Zusammenspiel der Komponenten ViPRO.gms und Cura die täglichen Abläufe sicher. Die im System integrierte Beschallungsanlage warnt die Personen im Gefahrenbereich und unterstützt durch gezielte akustische Informationen zum Fluchtweg bzw. zum korrekten Verhalten bei der Evakuierung.

Ganzheitliche Lösungen

Technische Hilfsmittel sind zur Bewältigung von Krisensituationen heute unerlässlich. Während klassische Gefahrenmanagementsysteme darauf ausgerichtet sind, technische Sub-Systeme zu überwachen und das Bedienpersonal im Störfall zu alarmieren, verfolgen die Entwickler der Funkwerk ViPRO.sys am Standort Leipzig einen anderen Ansatz: Sie setzen auf ganzheitliche Lösungen, um

◄◄ zurück zum Inhaltsverzeichnis

Auf einen Blick

ViPRO.gms

- PSIM-Software mit dezentraler Architektur gewährleistet hohe Ausfallsicherheit
- Modularer Aufbau für optimale Integration von kundenspezifischen Sub-Systemen
- Multimediale Benutzeroberfläche, inkl. sprachgestützter Bedienerführung und Alarmansage
- Vollständige Videounterstützung, inkl. IPTV
- Grenzenlose Kommunikationsmöglichkeiten via Telefon, Pager, E-Mail, PDA, Funk oder SMS

Cura

- Priorisierung von Ansagen nach ihrer Dringlichkeit, z. B. Unterbrechung einer laufenden Standardansage durch eine Notfalldurchsage
- Flexibles Eingreifen: Festlegung von Nutzern, die im Bedarfsfall Live-Durchsagen mittels GSM- oder über einen einfachen Festnetz-Anschluss tätigen können (Rollenkonzept)
- Archivierung aller Ansagen inkl. exaktem Zeitstempel, etwa für Qualitätskontrollen oder zum Nachweis von durchgeführten Ansagen
- Überwachung des gesamten Audiowegs zwischen den Eingängen und den Ausgangskreisen, zur Sicherstellung einer technisch einwandfreien Funktion
- Für große Betriebsstätten geeignet: bis zu acht Cura können zusammengeschaltet und somit 16 unabhängige Kreise betrieben werden

Mit der Beschallungsanlage Cura liefert Funkwerk die optimale akustische Ergänzung für das ViPRO.gms

das Management sicherheitskritischer Prozesse auf eine neue Stufe zu heben.

Für die Einbindung einer Videoanlage bedeutet dies beispielsweise, dass es den Sicherheitsdienst bereits dann alarmiert, wenn Kameraparameter auf einen möglichen Ausfall hindeuten. Es ist also gelungen, potenzielle Gefahrenquellen frühzeitig zu identifizieren, mögliche Störfälle klassifiziert an zentraler Stelle zu signalisieren und diese gegebenenfalls zu isolieren. Zudem stellt das System im Gefahrenfall eine effektive Unterstützung für den Anwender bei der Bearbeitung sicher, in dem es die bei der Implementierung hinterlegten Workflows vorgibt.

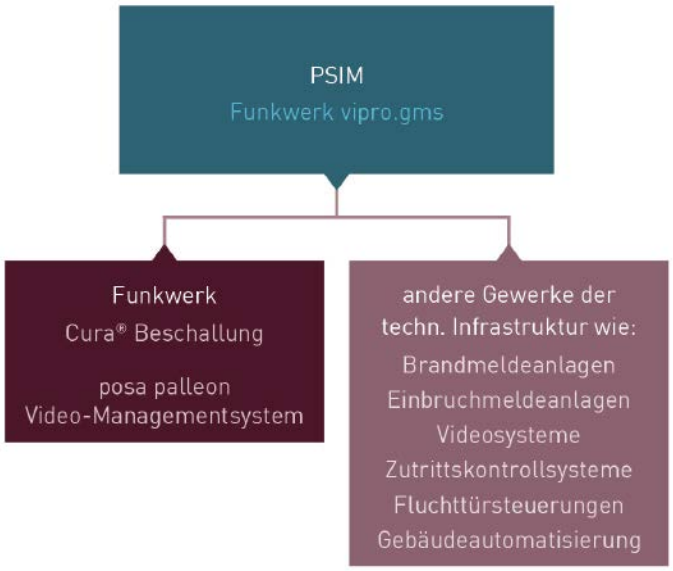
Diese zentrale Softwarelösung eignet sich insbesondere für Kritische Infrastrukturen, aber auch für Behörden sowie für Leitstellen bzw. Sicherheitszentralen in der Industrie. Mit dem System wird nicht nur die präventive Wartung und Instandhaltung der sicherheitsrelevanten Infrastruktur effizienter. Es ermöglicht auch eine zeitgerechte Wartung und Instandhaltung, sodass sicherheitsrelevante Systeme möglichst konstant zur Verfügung stehen.

PSIM-Software

Bei dem System handelt es sich um eine PSIM-Software (Physical Security Information Management). Sie ermöglicht das Anzeigen, Auswerten und Steuern verschiedener, dezentraler Sicherheitssysteme auf einer einzigen Plattform.

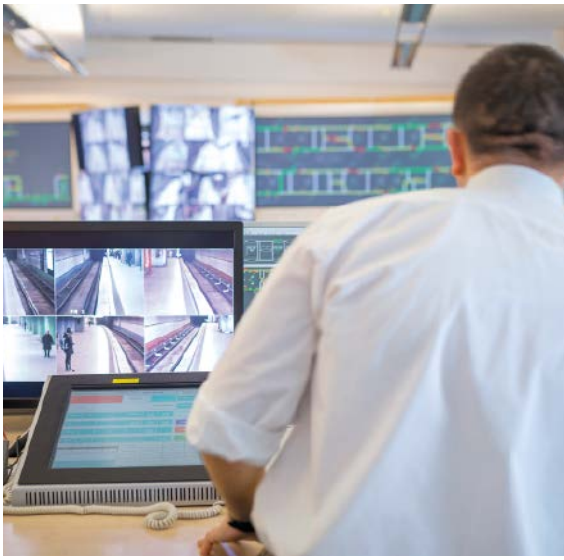
Bitte umblättern ▶

◀◀ zurück zum Inhaltsverzeichnis

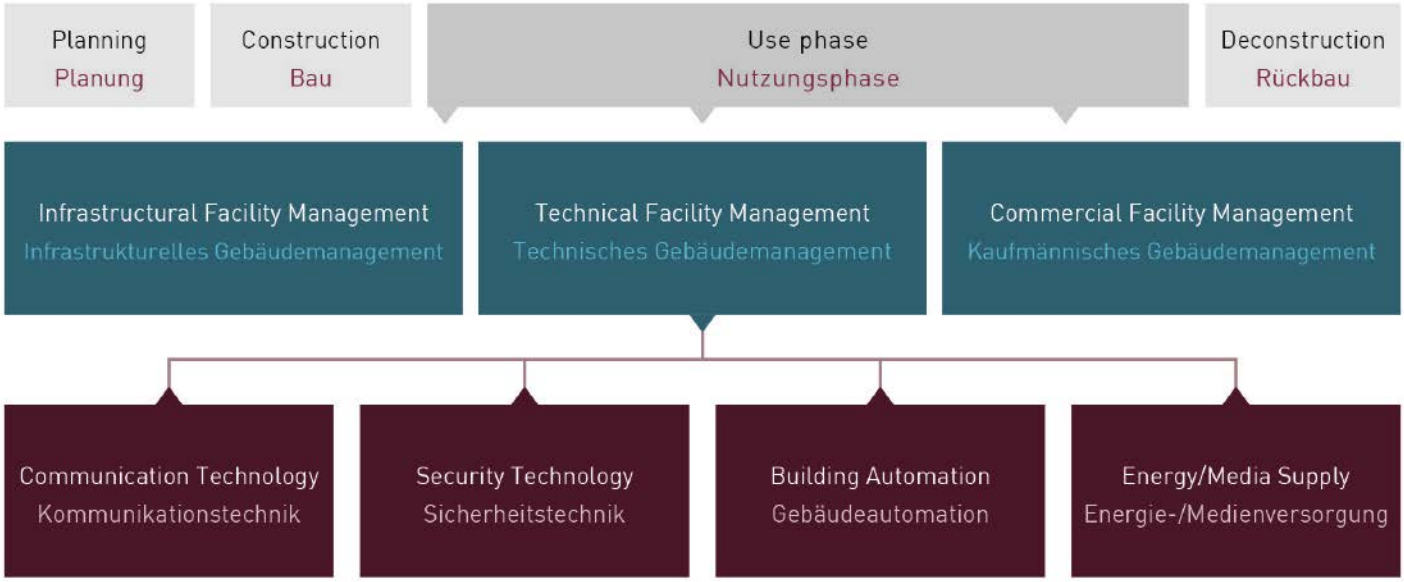


◀ Schematische Darstellung zur Integration von Sub-Systemen

Die Oberfläche ist intuitiv gestaltet und ermöglicht eine schnelle Einarbeitung der Benutzer ▶



▼ Cura Anwendungsmöglichkeiten



© Bilder: Funkwerk

Der Anwender kann von einem zentralen Standort agieren und überwacht alle integrierten Sicherheitsanwendungen, wie z. B. die Videoüberwachung, Zutrittskontrolle, Einbruch- und Brandmeldeanlagen oder die Zeiterfassung, übersichtlich auf einer Oberfläche. Alle Funktionen werden gebündelt angezeigt, was bei einem Alarm schnellere Reaktionszeiten ermöglicht.

Die Software ist in einer dezentralen Architektur konzipiert. Ein zentraler Server ist nicht erforderlich – alle Softwaremodule lassen sich auf verschiedenen Rechnern betreiben. Fällt eine Komponente aus, bleibt das Gesamtsystem davon unbeeinträchtigt, Teilfunktionen können sogar auf einzelne Bedienplätze ausgelagert werden. Dieser Aufbau ermöglicht eine gleichmäßige Lastenverteilung im Netz und gewährleistet eine hohe Ausfallsicherheit des Gesamtsystems.

Flexibilität dank modularem Aufbau

Das ViPRO.gms ist modular aufgebaut. Der Kunde entscheidet, welche individuellen Anforderungen für ihn wichtig sind. Das System wird entsprechend konfiguriert und kann jederzeit flexibel um weitere Komponenten und Funktionen erweitert werden und ist kosteneffizient. Auch der Anbindung von Sub-Systemen sind kaum Grenzen gesetzt.

Die Bedienung des Gefahrenmanagementsystems ist intuitiv gestaltet und unterstützt den Bediener aktiv bei der Bearbeitung von Meldungen durch individuell angepasste Workflows. Somit können Fehlerquellen in der Bedienung und bei der Bearbeitung von Meldungen deutlich reduziert werden. Der Anwender erhält u. a. eine vollständige Video-Unterstützung inkl. IPTV, kann Bild-in-Bild-Funktionen nutzen, die gewünschten Layer individuell ansteuern und auf sein Workflowmanagement zugreifen. Zudem verfügt das System über eine integrierte CAD-Engine (DWG, DXF) zum Einbinden von Lageplänen und einer Darstellung in beliebigen Zoom-Stufen. ●

Funkwerk vipro.sys GmbH
Leipzig
Tel.: +49 341 90222056
info@funkwerk.com
www.funkwerk.com

◀◀ zurück zum Inhaltsverzeichnis

KOMMENTAR

Vera Wolf zu EU-Richtlinie zum Schutz von KRITIS

Vera Wolf, Vice President of Sales, EMEA, von Zerto, einem Unternehmen von HPE, kommentiert die Folgen der jüngsten Direktive der EU. Um die kritischen Infrastrukturen der EU zu sichern, sei ein Schutz vor physischen und technologischen Angriffen erforderlich. Im November 2022 stimmte das Europäische Parlament über eine neue Richtlinie zur Verbesserung des Schutzes kritischer Infrastrukturen (KRITIS) in der EU ab. Die neuen Regeln zielen darauf ab, die Definition von kritischen Infrastrukturen zu harmonisieren, sodass sie in allen EU-Mitgliedstaaten einheitlich ist. In einer früheren KRITIS-Richtlinie fielen nur die Bereiche Energie und Verkehr in den Geltungsbereich der gemeinsamen Vorschriften.

© Zerto

Vera Wolf

Nun hat das Parlament den Anwendungsbereich erweitert und deckt die Sektoren Energie, Verkehr, Banken, Finanzmarktinfrastruktur, digitale Infrastruktur, Trink- und Abwasser, Lebensmittel, Gesundheit, öffentliche Verwaltung und Raumfahrt ab. Ziel der Richtlinie ist es, die Widerstandsfähigkeit der kritischen Systeme in der EU zu stärken und so die Sicherheit und das Leben der Europäer zu schützen. Mit der neuen Gesetzgebung soll sowohl auf die Herausforderungen der Klimakrise als auch auf die zunehmenden Sabotageakte in der Europäischen Union aufgrund des russischen Angriffskrieges gegen die Ukraine reagiert werden.

Digitale Infrastrukturen seien eine der vielen wichtigen Säulen, auf denen unser modernes Leben beruht. Es sei eine der wichtigsten Aufgaben von IT-Teams, diese Infrastrukturen rund um die Uhr und 365 Tage im Jahr am Laufen zu halten. Die potenziellen Bedrohungen reichen von physischen Angriffen bis zu fortschrittlichen Cyberangriffen. Widerstandsfähige Infrastrukturen sollten vor beidem abgesichert sein.

Um Rechenzentren vor physischen Angriffen zu schützen, benötigten Unternehmen Strategien zur Einrichtung einer geografischen Redundanz. Idealerweise sollten alle kritischen Rechenzentren und ihre wichtigen Workloads und Daten durch einen gespiegelten Standort gesichert sein, der die Aufgaben übernehmen kann, falls das Hauptrechenzentrum ausfällt. In der Vergangenheit waren dies vor allem regionale Naturkatastrophen. Mit der zunehmenden Bedrohung durch Sabotage schließt dies nun auch buchstäblich mögliche physische Angriffe von Menschenhand ein. Bei dem gespiegelten Back-up-Standort kann es sich um einen zweiten physischen Standort oder eine Cloud-basierte Infrastruktur handeln, wobei beide idealerweise mindestens 200 km vom Hauptstandort entfernt sind.

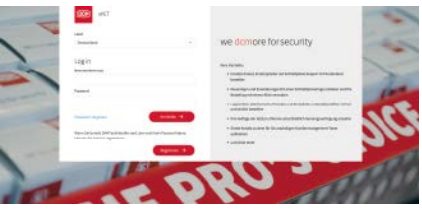
Angreifer müssen nicht unbedingt rohe Gewalt anwenden, um ein Rechenzentrum zu sabotieren. Cyberkriminelle haben seit Jahren bewiesen, dass sie in der Lage sind, ein Unternehmen in die Knie zu zwingen, indem sie es einfach mit Malware infizieren, zum Beispiel mit einem Ransomware-Angriff. Um ihre aktiven Workloads gegen solche Attacken zu schützen, müssen Unternehmen über Lösungen für Ausfallsicherheit verfügen, die die Workloads einfach auf den Back-up-Standort verlagern.

Die beste Option für eine geeignete BC/DR-Strategie wäre eine dedizierte Softwarelösung, die auf asynchroner Replikation und Continuous Data Protection (CDP) basiert und auf Hypervisor-Ebene läuft. Eine solche Lösung ist äußerst flexibel und in sehr kurzer Zeit, tatsächlich in Tagen, implementierbar, ohne dass in Hardware investiert werden müsste. Alles, was benötigt wird, ist ein sekundärer Standort, entweder physisch oder in der Cloud. Auf diese Weise können produktive Arbeitslasten einfach vom zweiten Standort aus ausgeführt werden, falls der Hauptstandort Opfer eines physischen oder eines Malware-Angriffs wird.

www.zerto.com

Händlerportal „eNet“

Das Händlerportal „eNet“ von Dom bietet den Käufern einige Vorteile: Beispielsweise können Ersatzschlüssel, Ersatzzylinder und Schließpläne bequem mit Kartenleser bestellt werden. Neuanlagen und Erweiterungen können mit einer Schließplanvorlage erstellt und die Bestellung dann mit einem Klick versendet werden (inkl. FastLane). Mit der Dom XL-Software (inkl. FastLane) werden Neuanlagen und Erweiterungen schnell und bequem erfasst und können per E-Mail bestellt werden. Digitale Schließsysteme, Lagerartikel und Einzelteile zu Handelsprofilen können über das Portal schnell und einfach bestellt werden. Die Aufträge der letzten drei Monate einschließlich Sendungsverfolgung sind einsehbar. Zudem ist es möglich, Kontakt zum zuständigen Kundenmanagement-Team aufzunehmen.



© Dom

Das eNet von Dom

www.dom-security.com

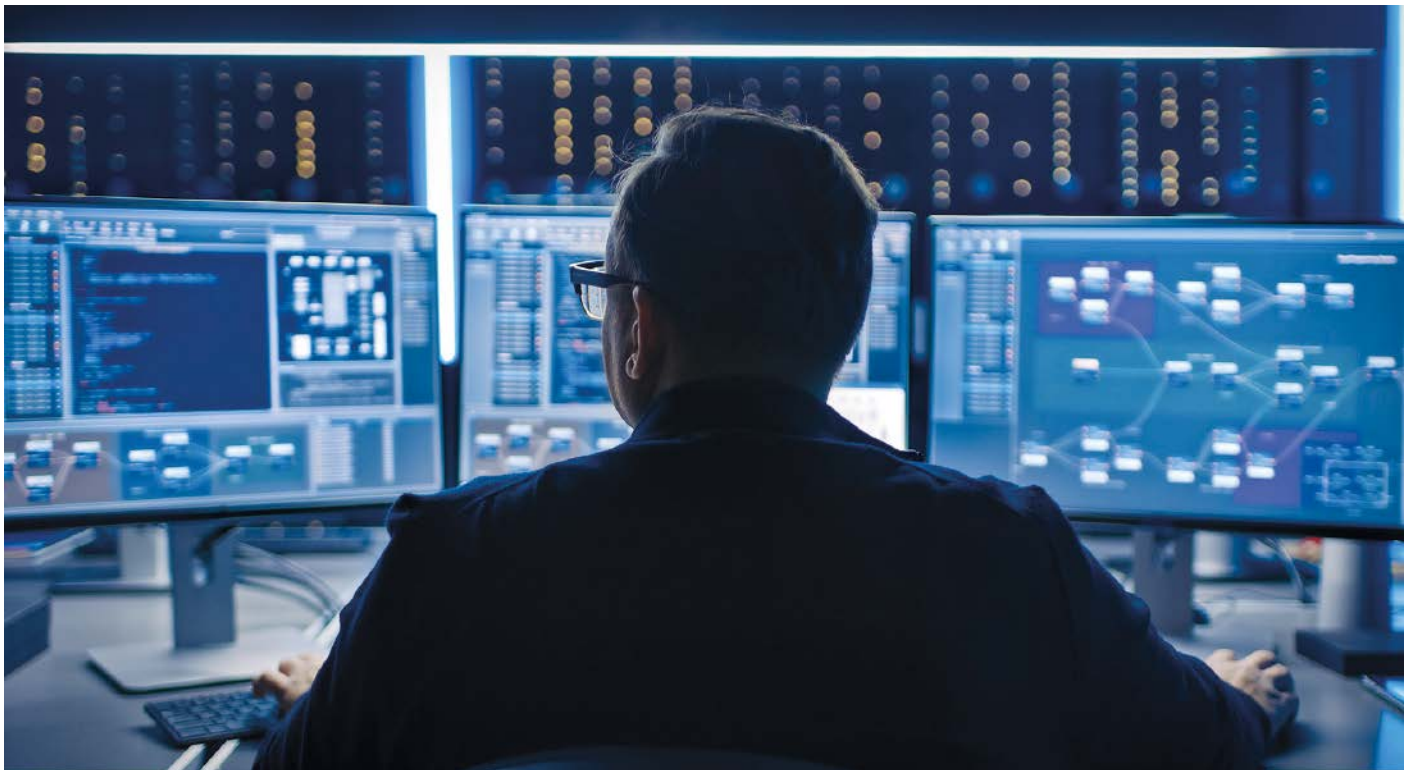
◄◄ zurück zum Inhaltsverzeichnis

CYBERSICHERHEIT

Kommandozentrale für mehr Cybersecurity

Angriffserkennung für KRITIS: Security Operation Center (SOC) as a Service

IT/OT-Infrastrukturen wirksam vor Cyberkriminalität zu schützen – dafür reicht Technik allein nicht. Um das komplexe Thema in den Griff zu bekommen, braucht es zusätzlich hochspezialisiertes Personal. Daran mangelt es vielen kleinen und mittelgroßen KRITIS-Betreibern. Diese Lücke können externe Security Operation Center füllen, die auch kostenmäßig eine interessante Alternative sind. Ein Beitrag von René Odermann, Account Director Development Cybersecurity bei Telent.



Datendiebstahl, Industriespionage oder Sabotage: Es ist keine Frage mehr, ob ein Unternehmen Opfer eines Cyberangriffs wird, sondern wann. 46 Prozent der von der Business Data Plattform Statista befragten deutschen Unternehmen haben im vergangenen Jahr mindestens einmal eine Cyberattacke erlebt. Die dadurch entstandenen Schäden summierten sich für die Gesamtwirtschaft auf mehr als 202 Milliarden Euro. Auch zukünftig wird das Gefahrenpotenzial – nicht zuletzt angesichts der geopolitischen Konflikte – weiter steigen. Security-Risiken zu verhindern, aufzudecken, zu bewerten, zu kontrollieren und im Fall der Fälle eine forensische Analyse einzuleiten sind die zentralen Aufgaben eines Security Operation Center (SOC). Es kombiniert technische Tools, strukturierte Prozesse sowie erfahrenen Experten und ist vergleichbar mit einer Kommandozentrale, in der innerhalb eines Unternehmens alle Fäden zum Thema Security zusammenlaufen.

IT-SiG 2.0 verschärft Pflichten für KRITIS-Betreiber

Die Bundesregierung will deutschlandweit die IT-Sicherheit erhöhen. Mit dem novellierten IT-Sicherheitsgesetz (IT-SiG 2.0) erweiterte sie deshalb den Kreis der KRITIS um die Branchen Abfallwirtschaft und Rüstungsindustrie sowie um Betriebe, die aufgrund ihrer Größe volkswirtschaftlich relevant sind, und deren wichtige Zulieferer. Sie alle verpflichtet das IT-SiG 2.0, ihre IT/OT-Umgebung besser gegen Cyberkrimi-

◀◀ zurück zum Inhaltsverzeichnis

nalität zu schützen, indem sie vom 1. Mai 2023 an Systeme zur Angriffserkennung, die dem „geltenden Stand der Technik“ entsprechen, ordnungsgemäß einsetzen und das gegenüber dem BSI nachweisen. Das IT-SiG 2.0 zielt gleichermaßen auf die IT und die Betriebstechnik (Operational Technology, OT). Denn sie steuert – ob bei der Stromversorgung, der Wasseraufbereitung oder in anderen kritischen Infrastrukturen – Prozesse, die sich bei Ausfall oder Manipulation duch einen Cyberangriff enorm auf die Versorgung und Sicherheit der Bevölkerung auswirken können. Im Zuge der Digitalisierung öffnet sich die ursprünglich von der Außenwelt abgeschottete OT und arbeitet immer enger mit der IT zusammen. Das schafft viele Angriffsflächen für Cyberattacken.

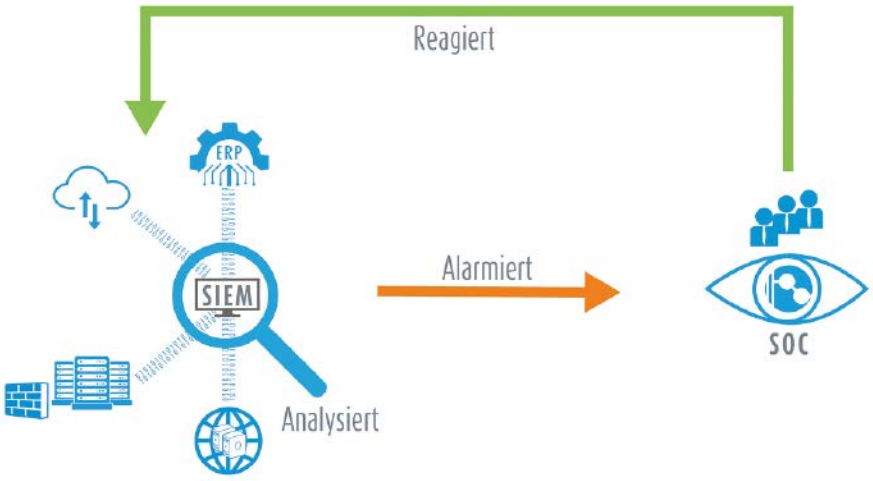
Das IT-SiG 2.0 lässt KRITIS-Unternehmen freie Hand für ein individuelles Konzept zur Angriffserkennung. Den Vorgaben entspricht u. a. ein System aus Intrusion Detection System (IDS) und Intrusion Prevention System

> „Die ursprünglich von der Außenwelt abgeschottete OT öffnet sich.“

(IPS). Ein auf die OT spezialisiertes IDS/IPS versteht die Sprache der proprietären Protokolle der Anlagen und Steuerungen und kann dadurch sowohl Angriffe als auch Fehlkonfigurationen, die auf menschlichem Versagen basieren, erkennen, im Verdachtsfall zu alarmieren oder nicht autorisierte Datenpakete zu blockieren. Eine Ergänzung hierzu sind Honeypots, die als virtuelle Maschinen bewusst mit Sicherheitslücken konfiguriert werden, um Hacker gezielt anzulocken und sie bewusst in die Irre zu leiten. Über die permanent überwachten Honeypots lassen sich IP-Adressen von Eindringlingen identifizieren, um sie dann für das gesamte System zu blockieren, und Informationen zur Vorgehensweise von Angreifern sammeln.

Echtzeit-Alarmierungen müssen qualifiziert bewertet werden

Die drei wichtigsten Funktionen einer Angriffserkennung sind Protokollierung, Detektion und Reaktion. Ein wichtiges Handwerkszeug, auch für das Team in einem SOC, ist ein SIEM. Die Abkürzung steht für Security Incident and Event Management und bezeichnet ein System, dass Meldungen, Logfiles und eine Vielzahl anderer



© Bilder: Telent

Bei einer 24/7-Netzwerküberwachung werten Experten im SOC die Alarmierungen des SIEM aus

Daten aus allen relevanten Bereichen der IT/OT-Infrastruktur sammelt, aggregiert und auf Auffälligkeiten hinweist. Um bei einer Alarmierung richtig zu reagieren, müssen die bereitgestellten Daten qualifiziert gesichtet und mit Blick auf die betriebliche Infrastruktur, etwa die verwendeten Softwareversionen, bewertet werden. In der Praxis kommen Fehlalarme häufig vor. Doch wer kann diese Aufgaben übernehmen? Angesichts begrenzter personeller und fachlicher Ressourcen stellt das viele Unternehmen vor große Herausforderungen; für die Umsetzung des IT-SiG 2.0 müssen sie noch höhere Hürde nehmen. Statt interne Kapzitäten aufzubauen, was auf dem leergefegten Arbeitsmarkt für Cybersecurity-Spezialisten kein einfaches Unterfangen ist, bieten sich externe Anbieter von Managed Security Services als Alternative an.

René Odermann, Account Director Development Cyber Security bei Telent

Unternehmen können mithilfe externer Dienstleister nur dann ein optimales Schutzniveau erreichen, wenn diese die richtigen Spezialisten an Bord haben. Dabei geht es nicht allein um die Zertifizierungen. Insbesondere bei komplexen IT/OT-Umgebung muss der Wissenshorizont passen, wie ihn Telent durch die langjährige Erfahrung in Industrial Security und industrieller Automatisation für KRITIS-Betreiber, Industrieunternehmen und öffentliche Auftraggeber besitzt. Dazu gehört für Telent auch, alle gesetzlichen Vorgaben mit ihren Muss-, Soll- und Kann-Kriterien detailliert zu betrachten, um konkret zu ermitteln, welche Punkte als Dienstleistungen erbracht werden können. Ein umfassender Sachverstand ist die Voraussetzung, um technisch hochwertige, verlässliche IT- und OT-Sicherheitsstrategien mit einem ganzheitlichen Cybersecurity-Ansatz umzusetzen.

Bei allem liegt der Fokus darauf, Technik in einen individuell für jeden Kunden sinnvollen Service zu überführen. Dabei nutzt das Telent-Team sein tiefgehendes OT-Verständnis, um außergewöhnlich flexible Lösungen zu finden, etwa vorhandene OT-Risikoerkennungsmodule von Unternehmen in die Dienstleistungen des SOC einzubinden. Als erfahrener Anbieter von Managed Security Services überwacht telent die Netzwerke seiner KRITS-Kunden rund um die Uhr, sucht aktiv nach Bedrohungen, entfernt diese und spricht weitergehende Handlungsempfehlungen aus. Somit füllt das externe SOC nicht nur Lücken bei knappen Personalressourcen, sondern stärkt die Cyberabwehr, ohne dass Unternehmen selbst hohe Investitionen in Securitysoftware, Hardware, Sicherheitsexperten, Schulungen und vieles mehr tätigen müssen, die beim Aufbau eines eigenen SOC entstehen. ●

Telent GmbH
Backnang
Tel.: +49 7191 900 0
Info.germany@telent.de
www.telent.de

◄◄ zurück zum Inhaltsverzeichnis

CYBERSICHERHEIT

Gestaffelte Abwehr

Klassische Ansatzpunkte für das Hacking Kritischer Infrastrukturen

In Zeiten geopolitischer Unsicherheit steht die IT von Betreibern Kritischer Infrastrukturen unter besonderem Fokus. Hacker verbessern ihre Attacken auf deren Betriebstechnik sowie auf Netzwerke und Systeme. Wer sich dagegen schützen will, darf sich aber nicht nur auf die Geräte für Steuerung und Kontrolle konzentrieren. Auch klassische IT-Endpunkte sind Teil der Angriffsfläche, die es zu schützen gilt. Abhilfe kann nur eine gestaffelte Abwehr bieten – auch mit einem erweiterten Blick auf einen erweiterten Katalog von Endpunkten. Ein Beitrag von Jörg von der Heydt, Regional Director DACH bei Bitdefender.

Die Kontrolle technischer Betriebsabläufe ist zentral für den Versorgungsauftrag Kritischer Infrastrukturen. Ein Angriff würde auf die Betriebstechnik (Operational Technology – OT), industrielle Kontrollsysteme (ICS) sowie die Supervisory-Control-and-Data-Acquisition- (SCADA) Hardware zielen. Eine solche Vorgehensweise verlangt von Hackern eine besondere Kenntnis dieser Systeme. Viele Administratoren in diesen Betrieben wiegen sich daher in einer vermeintlichen Sicherheit, weil sie glauben, dies sei weniger verbreitet oder Geräte seien vom Internet isoliert und damit geschützt. Doch dieser Schein trügt.

Gefahrenlage mit Unbekannten und Bekannten

Experten der NSA und des FBI warnen vor Attacken, die SCADA- und ICS-Systeme direkt angreifen. Die Entwickler und Betreiber von Advanced Persistent Threats (APT) erarbeiten sich mit zum Teil staatlicher Hilfe neue Cyberwar-Kompetenzen. Hintertüren in der klassischen IT können hier den Hackern den Weg eröffnen. Denn auch jenseits von OT und dem Internet of Things (IoT) gibt es lohnende und erreichbare Angriffsziele, die Betriebsabläufe unterbrechen können. Seit August 2021 beobachten Sicherheitsexperten komplexe Attacken auf die herkömmliche IT zur Industriespionage der Telekommunikationsindustrie im Mittleren Osten. Hierzulande wäre dies ein Angriff auf einen laut NIS 2.0 wichtigen KRITIS-Sektor. Höchstwahrscheinlicher Urheber der Kampagne ist die Advanced-Persistent-Threat (APT)-Gruppe Backdoor Diplomacy mit chinesischem Hintergrund. Am Beginn der Attacke stand eine unscheinbare Phishing-Mail – in der Folge nutzten die Hacker mit ProxyShell ein Gesamtpaket aus Malware-Funktionen gegen nicht gepatchte Microsoft-Exchange-Server. Sie umgingen Verfahren zur Authentifikation, eskalierten Privilegien digitaler gekaperter Identitäten und führten Remote Code aus. Das finale Ziel war die Datenexfiltration zu Spionagezwecken.

Hacker mit verschiedenen Motivationen agieren unterschiedlich. Von staatlichen Hintermännern gestartete Angriffe wollen so viel Schaden wie möglich erzeugen oder suchen nach Informationen. Interessanterweise steigt die Zahl von Angriffen auf intellektuel-

◄◄ zurück zum Inhaltsverzeichnis

les Eigentum weltweit, seit die chinesische Regierung den Made-in-China-2025-Plan für Entwicklung und Fortschritte in Schlüsselindustrien angekündigt hat. Für finanziell motivierte Täter haben KRITIS-Betreiber zudem ein hohes Lösegeldpotenzial: Krankenhäuser stehen unter hohem Druck, Pflege und Betrieb aufrechtzuerhalten und Menschenleben zu schützen. Dennoch lassen die Hacker Vorsicht walten: Seit dem Meilenstein der Attacke auf Colonial Pipeline greifen sie zurzeit prominenten Zielen augenscheinlich nicht an.

Wie sicher die Lage in Deutschland ist, lässt sich kaum sagen. Der Cyber-Kollateralschaden in Deutschland im Zuge des beginnenden Ukraine-Krieges im Februar 2022 sollte die Augen geöffnet haben: Eine Attacke auf den US-Satellitenbetreiber Viasat hatte damals dazu geführt, dass als Folge mindestens 3.000 Windräder in Deutschland für eine Fernwartung nicht mehr erreichbar waren. Der Fall zeigte, welchen Schaden Hacker aus Versehen verursachen können, indem sie IoT-Hardware wie Modems angreifen. Die Stromproduktion konnten sie nicht unterbrechen: Die Windräder waren aber ja auch nicht das Ziel.

KRITIS-IT-Infrastrukturen sind groß, komplex und schwer zu verwalten. Schäden, die nicht „nur“ Kundendaten als Beuteziel haben (aktuell T-Mobile in den USA) sind nur eine Frage der Zeit. Zahlreiche bekannte Übergriffe auf das Gesundheitswesen oder auf Kommunen wie Potsdam zeigen, dass Attacken den Betrieb länger unterbrechen können. Viele Verantwortliche haben ein Bewusstsein für diese Gefahren. Ihre Abwehr leidet aber unter dem Mangel an Zeit, Geld und Personal.

Jörg von der Heydt, Regional Director DACH bei Bitdefender

Gestaffelte Abwehr gegen gestaffelte Angriffe

Die Cyber-Abwehr muss sich in jedem Fall neu aufstellen. Das wird nicht ganz einfach. OT, SCADA und ICS erfordern sehr spezielle Schutzvorkehrungen. Solche Angriffe mögen seltener sein und bleiben, weil auch die Angreifer spezielle Kenntnisse mit sich bringen müssen. Im Einzelfall können sie jedoch verheerend sein.

Ebenso wichtig ist der Schutz der IT. Ein einfaches Spear Phishing kann einem SCADA-Administrator und seinen Rechten gelten. Solche Risiken frühzeitig zu erkennen und nachhaltig abzuwehren, ist unverzichtbar. Prävention, Erkennung und Abwehr verkürzen die Verweilzeit der Angreifer. Das ist zentral, denn Angriffe auf die KRITIS-IT sind selten opportunistische, sondern vielmehr geplante Feldzüge, die vor allem Zeit brauchen. Eine gestaffelte IT-Abwehrarchitektur oder ein Patch Management verkleinern die Angriffsfläche. Auch automatisierte Präventionsmechanismen helfen, Sicherheitsvorfälle zu vermeiden. Viele erpresserische Attacken starten über einfach Phishing-Mails, die sich bei hybriden Attacken zu weitreichenden Angriffen auswachsen können. Gerade wegen komplexer und langfristiger Charakteristika können die IT-Administrationen nicht auf Hilfe von außen durch z. B. externe Sicherheitsexperten (Managed Detection and Response Services eines SOC Teams) verzichten.

Die Angriffsszenarien sind unterschiedlich, KRITIS-IT ist komplex, die Hacker kreativ. Dennoch führt kein Weg daran vorbei, das Problem in den Griff zu bekommen. Das anstehende IT-Sicherheitsgesetz 3.0 oder die NIS-2-Vorgaben erhöhen den Druck und erlegen einem erweitertem Kreis von Unternehmen verschärfte Maßnahmen auf. Mehr Pflichten, Kontrollen und Strafen helfen jedoch nicht dabei, Lösungen zu finden – und zusätzliche Werkzeuge oder Finanzmittel werden nicht bereitgestellt. Am Ende geht es nicht nur darum, gesetzliche Vorgaben zu erfüllen, sondern die vorhandene Abwehr zu verbessern und zu stärken, um schwerwiegende und vor allem weitreichende Schäden zu verhindern. ●

Bitdefender GmbH
Schwerte
Tel.: +49 2304 945-160
info@bitdefender.de
www.bitdefender.de

VERKEHR / KRITIS

Feuer während der Fahrt

Löschkonzept für Schienenfahrzeuge: Brandbekämpfung im Technikraum

Wagner Rail ist eine Tochtergesellschaft der Wagner Group GmbH, die sich auf Brandschutzlösungen für Schienenfahrzeuge weltweit spezialisiert hat. Das Unternehmen hat nun eine Brandschutzlösung entwickelt, die in fahrenden Zügen Brände in offenen, stark durchlüfteten Technikbereichen löscht.


© mehaniq41 - stock.adobe.com

Die wirksame Brandbekämpfung in den stark durchlüfteten Technikbereichen – auch während der Fahrt mit hoher Geschwindigkeit und ohne, dass die Fahrt verlangsamt oder unterbrochen werden muss –, ist nach Angaben von Wagner weltweit bisher einzigartig. Wesentlicher Bestandteil von ganzheitlichen Brandschutzlösungen für Schienenfahrzeuge ist die Bekämpfung von Bränden in technischen Bereichen wie Transformatoren, Stromrichter oder Dieselmotoren. Diese Bereiche sind in der Regel mit mehreren nicht-verschließbaren Öffnungen ausgestattet, durch die die Belüftung erfolgt. Während der Fahrt entstehen somit Luftströmungen im Inneren dieser Technikbereiche. Für die wirksame Brandbekämpfung stellen diese Luftströmungen eine große Herausforderung dar. Bisher mussten Züge für eine sichere Brandlöschung die Geschwindigkeit verringern oder die Fahrt komplett unterbrechen.

Die Entwicklung des Löschverfahrens erfolgte auf Basis umfangreicher Testreihen, berichtet Peter Stahl, Geschäftsführer bei Wagner Rail: „In Zusammenarbeit mit dem Tüv Süd Rail sowie unter Einhaltung der Bahnrichtlinie ARGE Teil 2 ‚Brandbekämpfung in Schienenfahrzeugen' haben wir vom 15. bis 31. August 2022 eine umfangreiche Testreihe durchgeführt, bei der Brandszenarien unter verschiedenen Lüftungssituationen getestet wurden". Ziel der Tests sei es gewesen, Brände in technischen Bereichen des Zuges während der Fahrt vollständig zu löschen. Mit Hilfe der Testreihe habe man nachweisen können, dass simulierte Brände, die durch Fahrtwinde und seitlich auf den Zug wirkende Luftgeschwindigkeiten von über 100 km/h angefacht wurden, vollständig mittels Aerosollöschmittel gelöscht werden. ●

Wagner Group GmbH
Langenhagen
Tel: +49 511 97383 0
info@wagnergroup.com
www.wagnergroup.com

3 Fragen an …

… Dr. Peter Stahl, Geschäftsführer bei Wagner Rail


© Wagner Group GmbH

Dr. Peter Stahl, Geschäftsführer bei Wagner Rail

GIT SICHERHEIT: Herr Dr. Stahl, Sie haben gerade ein Verfahren zur Brandbekämpfung in fahrenden Zügen vorgestellt. Wie oft kommt es in deutschen Zügen oder auch andernorts vor, dass ein solches System gebraucht wird?
Peter Stahl: Immer dann, wenn Dieselaggregate oder Dieselmotoren auf Treibzügen oder Loks zu löschen sind, bei denen die Zuluftklappen auch im Brandfall nicht vollständig verschlossen werden können. Solche Dieselmotoren finden sich häufig auch auf Elektrolokomotiven oder Hybridfahrzeugen. Ohne unsere Lösung musste im Brandfall die Geschwindigkeit deutlich reduziert oder gar angehalten werden, was nicht in jeder Betriebssituation (z.B. Tunnelfahrten) wünschenswert ist.

Es geht ja um Technikbereiche in Zügen – hier facht die Belüftung eventuelle Brände regelrecht an. Ihre Lösung arbeitet mit Aerosollöschmitteln...?
Peter Stahl: Aerosole löschen durch Unterbrechung der Kettenreaktion des Verbrennungsprozesses. Unsere Lösung schafft es, die benötigte Löschmittelmenge von Menge und zeitlicher Abfolge so dimensioniert an potentielle Brandherde zu bringen, dass innerhalb weniger Sekunden die Feuer gelöscht werden. Die Versuche haben gezeigt, dass auch bei kontinuierlichem, nachträglichem Eintrag von Kraftstoff ein Wiederentzünden nicht mehr möglich ist.

Wann wird das System wo eingesetzt? Gibt es bereits Aufträge?
Peter Stahl: Aktuell sind moderne Triebzüge im Fokus und in der Angebotsphase.

◄◄ zurück zum Inhaltsverzeichnis

VdS-BrandSchutzTage 2022 mit Besucherrekord

Live-Vorführungen, Fachvorträge, lebendiger Austausch und Tausende Messe- und Fachtagungsbesucher prägten die VdS-BrandSchutz-Tage 2022. Die Freude, einander zum Netzwerken und Wissenstanken wiederzusehen, war auf den VdS-BrandSchutzTagen überall zu spüren. Über 4.000 Besucher aus dem In- und Ausland – das ist ein neuer Rekord – kamen in die Kölnmesse und besuchten die große Fachmesse mit ihren Attraktionen sowie die hochkarätigen Fachtagungen in den angrenzenden Sälen. Auf der großen Fachmesse zum vorbeugenden Brandschutz herrschte an beiden Messetagen reges Treiben. Viel besucht waren beispielsweise die Vorführung eines Niederdruck-Wassernebelsystems sowie der Stand des VdS-Brandmeldelabors, auf dem eine neue Laborprüfeinrichtung für CO-Melder in Aktion gezeigt wurde. Auf geführten Messerundgängen konnten die Besucher einen guten Überblick über interessante Neuheiten gewinnen. Eins der vielen vertretenen Themen waren Lithium-Batterien und ihre Brandgefahren.

© VdS/Martin Rottenkolber

An beiden Messetagen konnten Messebesuchende Live-Talks zu aktuellen Themen verfolgen

www.vds.de

Zertifizierter Brandschutz für industrielle Schaltschränke

Das Mini-Feuerlösch-System AMFE von Meister Automation GmbH schützt industrielle Schaltschränke und umschlossene Einrichtungen. Die unabhängigen Prüflabore der VdS Schadenverhütung GmbH haben nun die Zuverlässigkeit und Wirksamkeit gegenüber der Meister Automation GmbH bestätigt. Nun wurde die AMFE durch die VdS Schadenverhütung GmbH zertifiziert. Hergestellt wird das System von der Firma Job GmbH aus Ahrensburg. Die Meister Automation GmbH in Wertheim vertreibt das System exklusiv für die deutsche Industrie. Nach umfangreichen Tests könne die Zuverlässigkeit und Wirksamkeit des AMFE-Mini-Feuerlöschsystems für die S-&-R-AMFE mit Drucküberwachung bestätigt werden, so Heike Siefkes, Produktgruppenleiterin Gaslöschanlagen der VdS Schadenverhütung GmbH.

© Meister Automation

Automatische Mini-Feuerlösch-Einheit AMFE von Meister Automation

www.amfe.de

SONDERBRANDSCHUTZ

Bei erschwerten Bedingungen

Multitalent Ansaugrauchmelder in der Industrie

Brände in Industriegebäuden können nicht nur Sachschäden, sondern auch kostspielige Produktionsausfälle zur Folge haben. Das ist gerade bei Just-in-time-Produktion besonders kritisch, da bei Lieferunfähigkeit nicht nur Vertragsstrafen fällig werden können, sondern auch der Verlust von Kunden droht.

Überwachung von hohen Hallen ist für Ansaugrauchmelder kein Problem ▼

Die Herausforderung für den Brandschutz in Industriekomplexen liegt vor allem darin, dass sie viele Arbeitsbereiche mit unterschiedlichen Anforderungen unter einem Dach vereinen: Produktions- und Montagehallen, Lager, aber auch die Verwaltung einschließlich des Serverraums. Auf all dies braucht das Brandschutzkonzept eine gute Antwort, die den unterschiedlichen und anspruchsvollen Bedingungen gewachsen ist und eine möglichst frühe Detektion garantiert. Securiton Deutschland empfiehlt für diese Bereiche den Einsatz von Ansaugrauchmeldern, die mit einem umfangreichen Zubehör-Sortiment optimal den Anforderungen angepasst werden können.

Permanente Luftproben

In hohen Hallen und Lagern haben sich Ansaugrauchmelder zur Brandfrüherkennung durchgesetzt. Im Gegensatz zu punktförmigen Rauchmeldern werden bei Ansaugrauchmeldern Luftproben über mehrere Ansaugöffnungen permanent angesaugt und von hochempfindlichen Rauchsensoren in der Auswerteeinheit analysiert. Hierzu werden Ansaugleitungen verlegt, die eine flächendeckende Überwachung ermöglichen. Da die Luftproben jeweils von mehreren nebeneinanderliegenden Ansaugöffnungen aufgenommen werden, ergibt sich ein Kumulierungseffekt, welcher die Detektionsgeschwindigkeit weiter beschleunigt. Damit der Lagerbetrieb nicht während Revisionsarbeiten an der Brandmeldeanlage gestört wird, kann die Auswerteinheit des SecuriRAS ASD auch außerhalb der Gefahrenzone bzw. Überwachungsbereichs montiert werden.

zurück zum Inhaltsverzeichnis

Verschmutzte Umgebungen

Durch die Bearbeitung von Materialien, z. B. beim Schleifen und Schweißen, können in Produktionshallen verschiedene Staubarten zu Fehlalarm führen und die Ansaugleitungen verschmutzen. Securiton löst diese Problematik mit Filtereinheiten, die dem Ansaugrauchmelder vorgeschalten werden sowie in kritischen Anwendungen mit einer zusätzlichen automatischen Ausblasvorrichtung. Die Reinigung kann gemäß definierter Ausblaszyklen, bei Unterschreitung eines voreingestellten Luftstromwertes oder manuell erfolgen. In Umgebungen mit metallhaltigem Staub sollte der konventionelle Filter um ein zusätzliches Magnetfilter-System ergänzt werden. Denn metallhaltiger Staub hat eine Größenverteilung, die den Bereich von Rauchpartikeln überschneidet, sodass es konventionelle Staub-Filtereinheiten nicht möglich ist diese auszuscheiden.

Hochsensible Bereiche

Keine Frage: Ohne funktionierende IT-Infrastruktur würden viele Unternehmen stillstehen. Serverräume spielen eine zentrale Rolle. Sie vor Bränden zu schützen, ist eine komplexe Aufgabe, weil hohe und turbulente Luftströmungen die Früherkennung von verdünntem Rauch erschweren. In den meisten Fällen ist ein kleiner zylindrischer Trichter die richtige Lösung, um einen möglichst hohen Anteil der Luft auf Rauch zu überprüfen. Zu beachten ist weiter, dass mechanische Eingriffe zur Befestigung der Ansaugstellen in der Regel vom EDV-Gerätehersteller nicht erlaubt sind. Auch hier liefert Securiton eine Lösung: Der SecuriRAS ASD kann mittels Montageplatte ohne mechanische Eingriffe direkt außen am Schrank angebracht werden.

© Securiton Deutschland

> „Ansaugrauchmelder sind überall dort die richtige Wahl, wo punktförmige Melder umgebungsbedingt an ihre Grenzen stoßen.“

Sonderbrandmelder zentral verwalten

Das Multitalent Ansaugrauchmelder ist praktisch überall einsetzbar und mit dem passenden Zubehör auf jeden Sonderfall vorbereitet. Die jeweiligen Auswerteeinheiten kommunizieren dabei über eine Ringleitung direkt mit der Brandmeldezentrale. Die optionale und intelligente Vernetzungslösung Fides-Net lässt dabei die einzelnen Ansaugrauchmelder zu einem System mit zentraler Visualisierungs- und Bedienfunktion zusammenwachsen und ermöglicht die standortübergreifende Vernetzung der Brandmeldetechnik.

Dank der „Config over Line“-Funktion können Konfigurationen, Inbetriebnahme und Instandhaltung der Sonderbrandmelder bequem von der Brandmeldezentrale aus getätigt werden. Das hat deutliche Vorteile für Anlagenerrichter und Betreiber. Die zentrale Parametrisierung mehrerer Melder eliminiert Fehlerquellen und Revisionen können problemlos von einem einzigen Techniker erledigt werden. Zudem verringert sich der Instandhaltungsaufwand deutlich, denn die Wege zu den einzelnen Geräten entfallen. Alle Arbeiten werden effizient von der Brandmeldezentrale aus erledigt, ohne dabei den laufenden Betrieb zu beeinträchtigen. ●

Securiton Deutschland
Achern
Tel. +49 7841 6223-0
info@securiton.de
www.securiton.de

◄◄ zurück zum Inhaltsverzeichnis

GESUNDHEITSWESEN

Hört die Signale!

Sichere Vernetzung: Rufanlagen und IP

Rufanlagen sollen in Notsituationen Menschen, die sich selbst nicht helfen können, helfen. Nach DIN VDE 0834 müssen sie ein eigenes, von Fremdsystemen unabhängiges Leitungs- und Übertragungsnetz besitzen, dass durch die Geräte der Rufanlage überwacht und gesteuert wird. Die Ruffunktion hat höchste Priorität. Der ZVEI hat gerade sein Merkblatt zum Thema Rufanlagen und IP-Vernetzung in vollständig überarbeiteter zweiter Auflage vorgestellt. Es beschreibt die Risiken, die in Zusammenhang mit der Nutzung von systemfremden IT-Infrastrukturen entstehen können. Näheres erläutert Dr. Matthias Rychetsky, Mitautor des Merkblattes und Vorsitzender des Fachkreises Rufanlagen nach DIN VDE 0834 im ZVEI.

Dr. Matthias Rychetsky, Mitautor des Merkblattes und Vorsitzender des Fachkreises Rufanlagen nach DIN VDE 0834 im ZVEI

© ZVEI

GIT SICHERHEIT: Herr Dr. Rychetsky, eine Rufanlage zum Beispiel in einem Pflegeheim oder Krankenhaus wirkt immer auch mit der Informations- und Kommunikationstechnik (ITK) zusammen. Zur sicheren Vernetzung der beiden hat der ZVEI kürzlich ein Merkblatt herausgegeben. Ist das Verhältnis zwischen Rufanlage und ITK technologisch vielleicht ein wenig gespannt…?

Matthias Rychetsky: Keineswegs, aber es kommt darauf an, wie man mit der ITK umgeht, wo und wie man Schnittstellen zwischen Rufanlagen und ITK schafft und wie man diese behandelt und überwacht. Auf keinen Fall darf ein Signal einer Rufanlage, was ja in aller Regel ein Hilferuf eines Menschen ist, der sich nicht selbst helfen kann, verloren gehen. Daher muss die Ruffunktion höchste Priorität haben und jederzeit gewährleistet sein. Das ist unter allen Umständen zu berücksichtigen und prägt das Verhältnis der Rufanlagen zur ITK im Krankenhaus, Pflegeheim oder wo auch immer Rufanlagen eingesetzt werden.

Sie haben das Zusammenwirken in einem neuen ZVEI-Merkblatt „Rufanlagen nach DIN VDE 0834 und IP-Vernetzung“ dargelegt. Was sind die wichtigsten Inhalte?

Matthias Rychetsky: Zentrale Aspekte der DIN VDE 0834 sind zum einen die funktionale Sicherheit, gewährleistet z. B. durch eine laufende und selbständige Störungsüberwachung und die Einschränkung der Nutzung systemfremder Übertragungswege. Zum anderen geht es um die elektrische Sicherheit zum Schutz des Patienten insbesondere die elektrische sichere Trennung der Stromkreise nach EN 60601-1 mit 2 x MOPP der Rufanlage gegenüber anderen Systemen und dem Versorgungsnetz. Das Merkblatt geht insbesondere auf die Nutzung von Übertragungswegen anderer Systeme ein, da das nach DIN VDE 0834 in der Regel nicht zulässig ist.

Wie genau kann das umgesetzt werden?

Matthias Rychetsky: Ideal ist ein eigenes von anderen Systemen unabhängiges Leitungsnetz der Rufanlage. Daran dürfen nur durch den Hersteller der Rufanlage freigegebene Geräte angeschlossen werden. Schnittstellen müssen elektrisch und funktional sicher sein. Unter sehr streng abgegrenzten Bedingungen, wie etwa einem kontinuierlichen Risikomanagement, dürfen zwischen zusammenhängenden organisatorischen Einheiten der Rufanlage, sogenannten Organisationsgruppen, und externen Gewerken Übertragungswege von Fremdsystemen eingesetzt werden. Innerhalb der Organisationsgruppen der Rufanlage ist dies definitiv ausgeschlossen. Selbstverständlich ist es komplett unzulässig, die einzelnen Geräte der Rufanlage über die allgemeine IT-Infrastruktur miteinander zu verbinden. Diese Zusammenhänge haben wir in praxisnahen Schaubildern erläutert, aus denen der Planer und Praktiker erkennen kann, welche technischen und organisatorischen Konstellationen zwischen Rufanlage und allgemeiner ITK zulässig sind und welche nicht.

Eine Kopplung von Radio oder Fernsehen im Kranken- oder Pflegezimmer mit der Rufanlage ist technisch also unzulässig?

Matthias Rychetsky: So pauschal trifft das nicht zu. Die zulässigen und unzulässigen Konstellationen werden in unserem Merkblatt präzise dargelegt. An die Rufanlage dürfen nur durch den Hersteller der Rufanlage freigegebene Geräte angeschlossen werden. Das Anschließen anlagenfremder Geräte ist nur dann möglich, wenn eine Beeinträchtigung der Rufanlage und eine Gefährdung des Patienten oder Bewohners ausgeschlossen werden kann. Dieses Prinzip heißt Rückwirkungsfreiheit – die Funktion der Rufanlage darf auf keinen Fall gefähr-

◄◄ zurück zum Inhaltsverzeichnis

det werden. Bei einer Integration von Mehrwertdiensten in die Rufanlage via Anschlussstecker oder Endgerät sind die Normvorgaben, insbesondere bezüglich Isolation, sowie die funktionale und elektrische Sicherheit der Rufanlage zu beachten.

Welche organisatorischen Aspekte sehen Sie für den normenkonformen Betrieb einer Rufanlage?

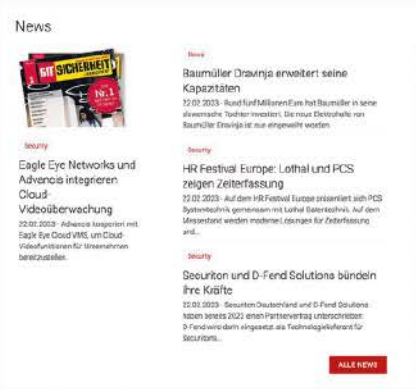
Matthias Rychetsky: Neben der Technik spielen auch betrieblich-organisatorische Zusammenhänge für die Funktionalität einer Rufanlage eine wichtige Rolle. Das beginnt mit der eindeutigen Kennzeichnung von Anschlussdosen, Patchkabeln und Patchfeldern, um die verwechslungsfreie Zuordnung zur Rufanlage dauerhaft zu gewährleisten. Bei der Zusammenlegung von Abteilungen im Nacht- oder Wochenend-Betrieb ist darauf zu achten, dass innerhalb der Organisationsgruppe – als kleinste von einer einzelnen Person betreubare Einheit – das beschriebene unabhängige Leitungsnetz nicht verletzt wird. Und schließlich gibt die Norm DIN VDE 0834 die regelmäßige Überprüfung der Rufanlage vor. ●

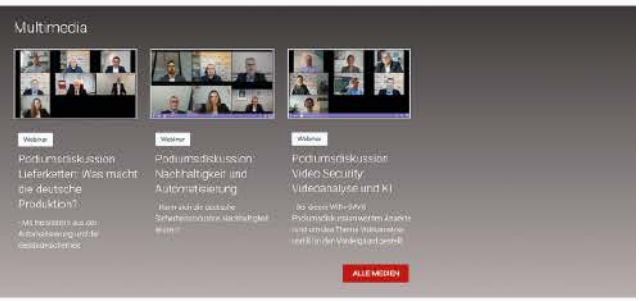
Hier finden Sie das komplette ZVEI-Merkblatt:
https://bit.ly/3I6zKz6

ZVEI e.V.
Frankfurt am Main
Tel.: +49 69 6302 272
peter.krapp@zvei.org
www.zvei.org

◀◀ zurück zum Inhaltsverzeichnis

DIESEN MONAT AUF GIT-SICHERHEIT.DE





IMPRESSUM

Herausgeber
Wiley-VCH GmbH

Geschäftsführer
Sabine Haag, Dr. Guido F. Herrmann

Publishing Directors
Dipl.-Betriebswirt Steffen Ebert
Dr. Heiko Baumgartner

Wissenschaftliche Schriftleitung
Dipl.-Verw. Heiner Jerofsky (1991–2019) †

Anzeigenleitung
Miryam Reubold
+49 6201 606 127

Commercial Manager
Jörg Wüllner
+49 6201 606 748

Redaktion
Dr. Heiko Baumgartner
+49 6201 606 703
Dipl.-Betrw. Steffen Ebert
+49 6201 606 709
Matthias Erler ass. iur.
+49 6129 50 25 300
Dr. Timo Gimbel
+49 6201 606 049
Stormy Haust
+49 6201 606 125
Lisa Holland M.A.
+49 6201 606 738
Eva Kukatzki
+49 6201 606 761

Textchef
Matthias Erler ass. iur.
+49 6129 50 25 300

Herstellung
Jörg Stenger
+49 6201 606 742
Claudia Vogel (Anzeigen)
+49 6201 606 758

Satz + Layout Ruth Herrmann
Lithografie Elke Palzer

Sonderdrucke
Miryam Reubold
+49 6201 606 172

Wiley GIT Leserservice (Abo und Versand)
65341 Eltville
Tel.: +49 6123 9238 246
Fax: +49 6123 9238 244
E-Mail: WileyGIT@vuservice.de
Unser Service ist für Sie da von Montag - Freitag zwischen 8:00 und 17:00 Uhr

Wiley-VCH GmbH
Boschstr. 12, 69469 Weinheim
Telefon +49 6201 606 0
E-Mail: git-gs@wiley.com
Internet: www.git-sicherheit.de

Verlagsvertretung
Dr. Michael Leising
+49 36 03 89 42 800

Bankkonten
J.P. Morgan AG, Frankfurt
Konto-Nr. 6161517443
BLZ: 501 108 00
BIC: CHAS DE FX
IBAN: DE55501108006161517443

Zurzeit gilt Anzeigenpreisliste vom 1.1.2022. Die namentlich gekennzeichneten Beiträge stehen in der Verantwortung des Autors.

2023 erscheinen 10 Ausgaben
„GIT SICHERHEIT"
Druckauflage: 25.000
inkl. GIT Sonderausgabe PRO-4-PRO

Abonnement 2023: 10 Ausgaben (inkl. Sonderausgaben) 118,00 €, zzgl. MwSt. Einzelheft 16,30 € zzgl. Porto + MwSt. Schüler und Studenten erhalten unter Vorlage einer gültigen Bescheinigung einen Rabatt von 50 %. Abonnement-Bestellungen gelten bis auf Widerruf; Kündigungen 6 Wochen vor Jahresende. Abonnementbestellungen können innerhalb einer Woche schriftlich widerrufen werden, Versandreklamationen sind nur innerhalb von 4 Wochen nach Erscheinen möglich.

Alle Mitglieder der Verbände ASW, BHE, BID, BDSW, BDGW, PMeV, Safety Network International, vfdb und VfS sind im Rahmen ihrer Mitgliedschaft Abonnenten der GIT SICHERHEIT sowie der GIT Sonderausgabe PRO-4-PRO. Der Bezug der Zeitschriften ist für die Mitglieder durch Zahlung des Mitgliedsbeitrags abgegolten.

Druck
westermann DRUCK | pva
Printed in Germany, ISSN 0948-9487

PEFC zertifiziert
Dieses Produkt stammt aus nachhaltig bewirtschafteten Wäldern und kontrollierten Quellen
PEFC/04-31-0714
www.pefc.de

WILEY

◄◄ zurück zum Inhaltsverzeichnis

WILEY

NEUE PLATTFORM

Wiley Industry Days

WIN DAYS

14.–16. März 2023

www.WileyIndustryDays.com

Mit renommierten Speakern – unter anderem:

Dr. Gunther Kegel, CEO Pepperl+Fuchs Group, Präsident des ZVEI

Frank Eberle, Advanced Development, Network Systems, PILZ

Steffen Zimmermann, Leiter Competence Center Industrial Security, VDMA

VIRTUELLE KONFERENZ ZUM THEMA: Corporate Resilience – Konzepte und Lösungen gegen Angriffe und Gefahren

JETZT KOSTENFREI ALS BESUCHER ANMELDEN
WileyIndustryDays.com

Organisationsteam:

Lisa Holland
+49 6201 606 738
lisa.holland@wiley.com

Dr. Heiko Baumgartner
+49 6201 606 703
heiko.baumgartner@wiley.com

Dr. Timo Gimbel
+49 6201 606 049
timo.gimbel@wiley.com

Jörg Wüllner
+49 6201 606 749
joerg.wuellner@wiley.com

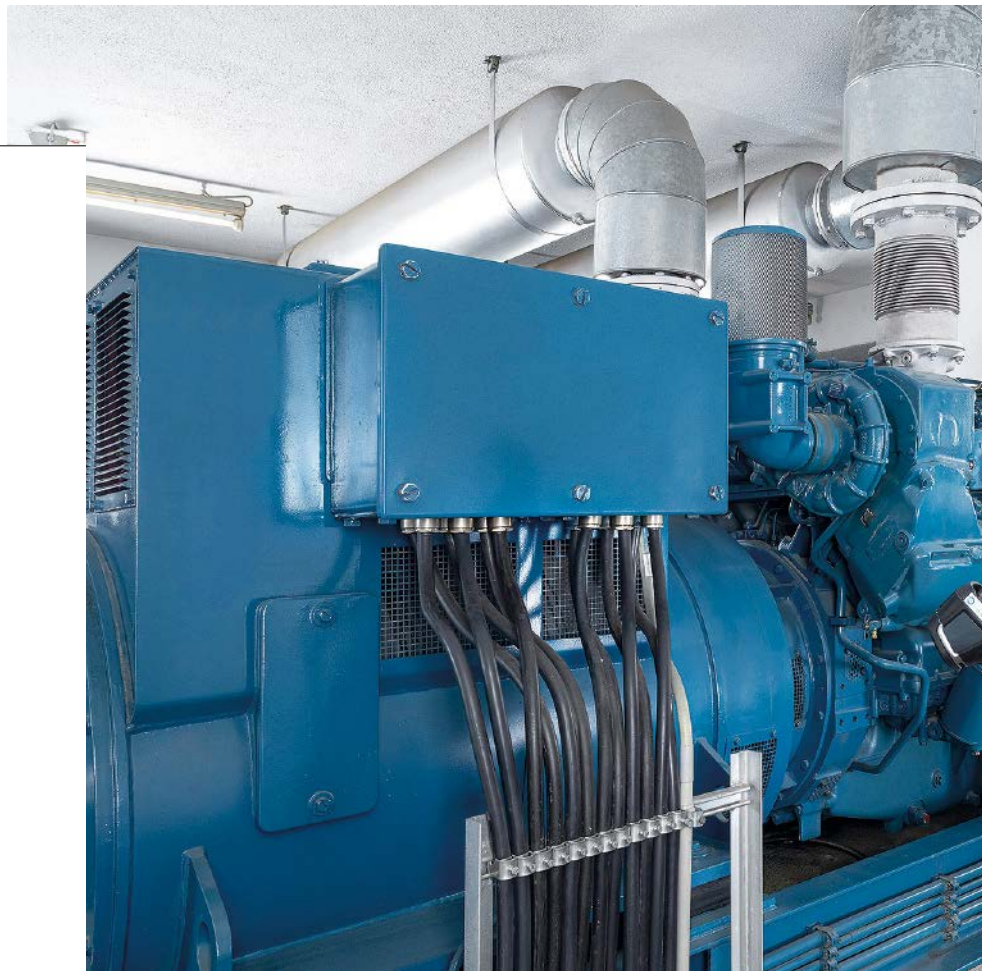
Miryam Reubold
+49 6201 606 127
miryam.reubold@wiley.com

Dr. Michael Leising
+49 3603 89 42 800
leising@leising-marketing.de

Steffen Ebert
+49 6201 606 709
steffen.ebert@wiley.com

GIT SICHERHEIT

GIT SECURITY EMEA



THERMOGRAFIE

Die Hitze im Blick

Elektrik im laufenden Betrieb prüfen mit Thermografie

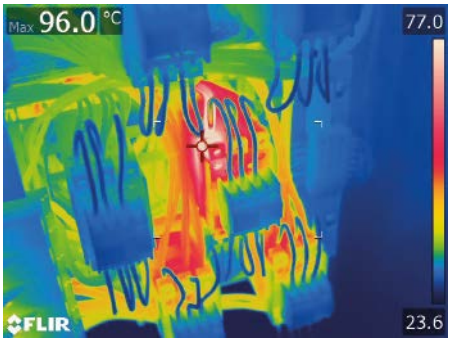
Um elektrische Anlagen zu prüfen, müssen sie meist abgeschaltet und der Betrieb unterbrochen werden. Nicht so bei der Elektrothermografie. Sie erfolgt im laufenden Betrieb und macht damit auch die tatsächlichen Betriebszustände bei Belastungen sichtbar.

Ein Drittel aller Brände in Deutschland ist auf eine mangelhafte Elektrik zurückzuführen. Gesetzgeber, Berufsgenossenschaften und Versicherungsgeber fordern deshalb von den Gebäudeeigentümern und -betreibern, elektrische Anlagen und Betriebsmittel regelmäßig prüfen zu lassen. Davon profitieren auch Eigentümer, Betreiber und Nutzer von Gebäuden oder Industrieanlagen. Grundlegende Vorgaben machen unter anderem die DGUV (Deutsche Gesetzliche Unfallversicherung), die Betriebssicherheitsverordnung, das Baurecht der Länder sowie der GdV (Gesamtverband der Deutschen Versicherungswirtschaft) über die Prüfrichtlinien des VdS.

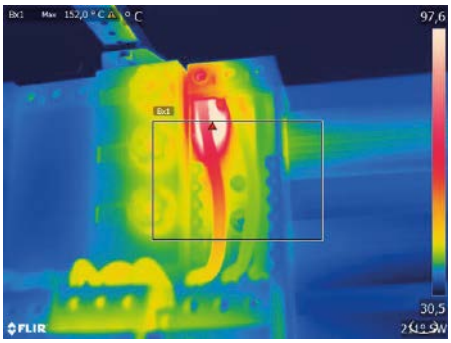
Sicherheit für Mitarbeitende und Prüfende

Übliche Prüfverfahren liefern keine absolut verlässlichen, ganzheitlichen Aussagen über den Zustand elektrischer Installationen – vor Allem in Bezug auf das Verhalten bei hohen Belastungen. Das Problem: Für die gängigen Methoden muss die Anlage abgeschaltet bzw. vom Strom genommen werden. Prüfungen werden deshalb meist in Betriebsunterbrechungen und Produktionspausen durchgeführt. Dabei herrschen jedoch zumeist keine realistischen Betriebsbedingungen. Eventuelle betriebsbedingte Überlasten, Erwärmungen aufgrund hoher Gleichzeitigkeitsfaktoren oder erhöhter Umgebungstemperaturen aufgrund von Prozess- oder Anlagenabwärme bleiben unberücksichtigt oder werden vom Prüfpersonal nicht sicher erkannt.

Insbesondere für Feuerversicherungen ist in der Regel eine VdS-Prüfung bzw. Schutzklauselprüfung obligatorisch. Dabei fordern immer mehr Versicherungsgeber zusätzlich zur konventionellen Prüfung nach SK 3602 (VdS-Prüfung der Elektrischen Anlage) eine thermografische Untersuchung durch anerkannte Elektrothermografen nach VdS 2859. Dabei macht eine Wärmebildkamera die Temperaturen elektrischer Anlagen anhand der Infrarotstrahlung sichtbar. Thermogramme bilden die Temperaturverteilungen ab. Das alles erfolgt durch ausgebildete Experten der Elektrothermografen, die die Wärmebilder mit geschultem Blick auf Plausibilität und mögliche Auffälligkeiten hin bewerten können. Das gelingt im laufenden Betrieb – selbst unter Spitzenlasten. So lassen sich unsichtbare Defekte und Gefahrenstellen anhand ihrer thermischen Unregelmäßigkeiten frühzeitig lokalisieren.



Das Thermogramm macht Dinge sichtbar, die dem Auge sonst verborgen bleiben – wie hier, eine thermische Überlastung durch einen fehlerhaften Leiteranschluss.



Thermogramme bilden die Temperaturverteilungen ab und ermöglichen so das Auffinden von Auffälligkeiten

◄◄ zurück zum Inhaltsverzeichnis

◀ Thermografische Untersuchungen gelingen im laufenden Betrieb – selbst unter Spitzenlasten

Beispielsweise lassen sich Materialverschleiß oder sonstige Alterungsschäden erkennen und ausbessern, bevor sie die Leistung der Anlage signifikant einschränken. Ein Kühlmanagement lässt sich mithilfe der Wärmebilder gut analysieren. Bei Neuanlagen werden mögliche Installationsfehler sichtbar und ihre Zuverlässigkeit und Verfügbarkeit werden verbessert. So haben die Prüferinnen und Prüfer schon mangelhafte Klemmstellen, Kabelanschlüsse oder Isolierungen bei der Inbetriebnahme einer Anlage aufgedeckt. Die Elektrothermografie ist berührungslos und reduziert auch das Unfallrisiko bei der Prüfung.

Expertise macht den Unterschied

Viele Elektrofachbetriebe bieten eine Untersuchung elektrischer Anlagen mit Infrarotkameras an. Bereits einfache Prüfungen erhöhen die Sicherheit, wenn damit etwa eklatante Fehlstellen erkannt werden – zumal sie mit wenig Zeit- und Kostenaufwand verbunden sind. Die geforderten elektrothermografischen Untersuchungen der Anlage nach VdS 2858 ersetzen sie aufgrund der Detailtiefe und des Umfangs der Untersuchung indes nicht.

Hierfür ist der Einsatz moderner Hochleistungsgeräte durch spezialisierte und zertifizierte Elektrothermografen erforderlich. Mit einer fundierten Ausbildung und einschlägiger Erfahrung sind sie in der Lage, die Feinheiten thermografischer Bilder zu erkennen und richtig zu interpretieren. Reflektierende Temperaturen beispielsweise können Aufnahmen verzerren. Das ist für ungeschulte Mitarbeitende bisweilen nicht ersichtlich, was zu fehlerhaften Ergebnissen führen kann.

Zur persönlichen Expertise kommt die eingesetzte Technik: Spezialisierte Software und Rechenmethoden ermöglichen, die Prüfergebnisse an verschiedene Betriebsbedingungen anzupassen und auf besondere Auslastungen und Umgebungsbedingungen zu skalieren. Damit ist der Lastzustand der Anlage bei der Prüfung nicht alleinig ausschlaggebend für das Prüfergebnis. Stattdessen können die Fachleute mit ihrer Erfahrung, High-Tech-Ausrüstung und angepasster Computertechnik ganzheitliche Prüfaussagen für alle erwartbaren Betriebszustände treffen. Prädikativ kann hier beispielsweise untersucht werden, was passiert, wenn die Anlage im Hochsommer bei Temperaturen um 40 °C unter Volllast betrieben wird.

Der abschließende Prüfbericht beschreibt mögliche Mängel und Auffälligkeiten eindeutig und klar verständlich, gegebenenfalls ergänzt um Ursachenbeschreibungen. Die Ergebnisse kommen in Papierform oder online als elektronisches Prüfbuch.

Technische und rechtliche Risiken reduzieren

Die elektrothermografische Prüfung vermeidet Anlagenstillstände und damit kostenintensive Betriebsunterbrechungen. Sie ermöglicht eine wirksame, vorausschauende Instandhaltung (Predictive Maintenance) und ergänzt bestehende Prüfmethoden und lebenszyklusbasierte Wartungs- und Instandhaltungskonzepte um eine neue sicherheitsfördernde Komponente. Anlagen- und Gebäudebetreiber erfüllen nicht zuletzt die Vorgaben ihrer Feuerversicherer, verbessern die Sicherheit ihrer Mitarbeitenden und ihrer Assets. Damit schützen sie ihr Unternehmen auch gegen mögliche Haftungsfragen im Schadensfall. ●

Autor
Stefan Veit
Leiter Produkt- und Qualitätsmanagement
im Geschäftsfeld Elektro- und
Gebäudetechnik, Bereich Elektrotechnik
Tüv Süd Industrie Service GmbH

Tüv Süd Industrie Service GmbH
Geschäftsfeld Elektro- und Gebäudetechnik
München
Tel.: +49 89 5791-4394
e-thermografie@tuvsud.com
tuvsud.com/de-is

Rose+Krieger weiter auf Wachstumskurs

Mit einer Umsatzsteigerung gegenüber dem Vorjahr war das Jahr 2022 für Rose+Krieger überdurchschnittlich erfolgreich. Auch für 2023 plant das Unternehmen vorsichtig optimistisch mit einem moderaten Wachstum. Als einen Motor des Erfolgs sieht Geschäftsführer Dr. Gregor Langer den Geschäftsbereich Systemlösungen. Man sei mehr als erfreut darüber gewesen, trotz der zahlreichen Herausforderungen in 2022 – darunter Corona, gestörte Lieferketten und Materialmangel – ein Umsatzplus verzeichnen zu können, das deutlich über der ursprünglichen Planung lag, so Dr. Gregor Langer. Verantwortlich für den Erfolg sei laut Langer vor allem das Systemgeschäft und dort insbesondere der Bereich Lean Solutions für Montagearbeitsplätze. Daher seien Lean Solutions neben der Geschäftsentwicklung in den Branchen Intralogistik und Verpackung eines unserer zentralen Fokusthemen in diesem Jahr, sagt Gregor Langer und verweist auf die umfassenden Kompetenzen des Unternehmens in diesen Segmenten.

www.rk-rose-krieger.com

Dr. Gregor Langer, Geschäftsführer von RK Rose+Krieger

◀◀ zurück zum Inhaltsverzeichnis

MASCHINEN- UND ANLAGENSICHERHEIT

Funktionale Sicherheit – Manipulationen an Schutzeinrichtungen vorbeugen

Werden Schutzeinrichtungen an Maschinen außer Kraft gesetzt, steigt die Gefahr für Arbeitsunfälle. Insbesondere während der Instandhaltung beim Betreiber werden Schutzeinrichtungen an Maschinen häufig manipuliert, zum Beispiel wenn der bereitgestellte Funktionsumfang für bestimmte Tätigkeiten nicht ausreicht oder Schutzeinrichtungen als störend empfunden werden.

Die Artikel-Serie in Kooperation von VDMA Elektrische Automation und GIT SICHERHEIT beleuchtet Ursachen und Hintergründe. Sie zeigt die aktuellen gemeinsamen Anstrengungen von Maschinenherstellern und Automatisierungslieferanten im VDMA in enger Zusammenarbeit mit Maschinenbetreibern und Berufsgenossenschaften auf dem Weg zu praktikablen Lösungen für mehr Sicherheit bei weniger Engineering-Aufwand.

VDMA-Ansprechpartner: Birgit Sellmaier betreut im VDMA-Fachverband Elektrische Automation Technik- und Technologiethemen wie Steuerungstechnik und Funktionale Sicherheit in der Anwendung im Maschinenbau.

VDMA Elektrische Automation
birgit.sellmaier@vdma.org
Tel.: +49 69 6603 1670
https://www.vdma.org/elektrische-automation

Kooperationspartner:

VDMA Elektrische Automation

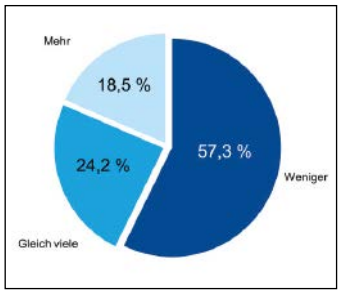
GIT SICHERHEIT

© Michael Hüter

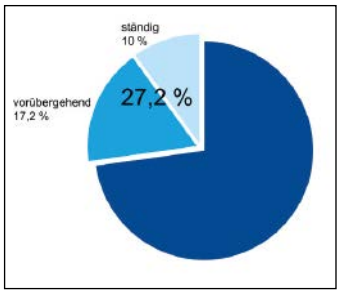
Ergebnisse der aktuellen IFA-Erhebung „Manipulation von Schutzeinrichtungen“

Häufig sind es die an den Maschinen und Anlagen arbeitenden Personen selbst, die Schutzeinrichtungen manipulieren. Dabei sollen diese Schutzeinrichtungen eben genau jene Personen vor Gefährdungen schützen. Doch nicht selten werden Schutzeinrichtungen aus Sicht der Bediener in erster Linie als störend oder hinderlich bei der Bedienung wahrgenommen, weshalb sie überbrückt oder einfach gleich abmontiert werden. Um besser zu verstehen, wie verbreitet das Phänomen ist und wie genau es sich manifestiert, hat das Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA) zwischen den Jahren 2020 und 2022 eine Umfrage durchgeführt, an der sich über 840 Personen beteiligt haben – mehrheitlich Fachkräfte für Arbeitssicherheit. Stefan Otto, Prüfingenieur Funktionale Sicherheit im IFA und Leiter des Arbeitskreises Manipulation von Schutzeinrichtungen der DGUV, hat für uns die Ergebnisse der Umfrage zusammengefasst und erläutert.

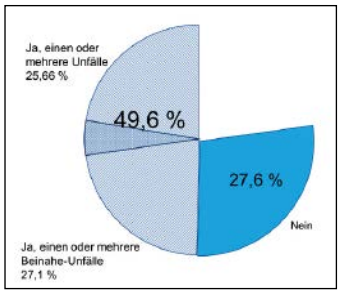
zurück zum Inhaltsverzeichnis



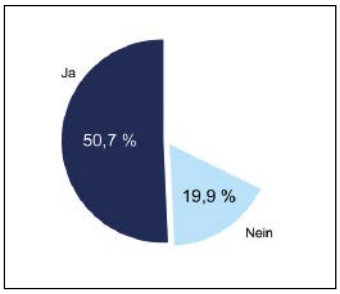
Ergebnis auf die Frage: „Werden Ihrer Einschätzung nach heute mehr oder weniger Maschinen manipuliert als vor zehn Jahren?“



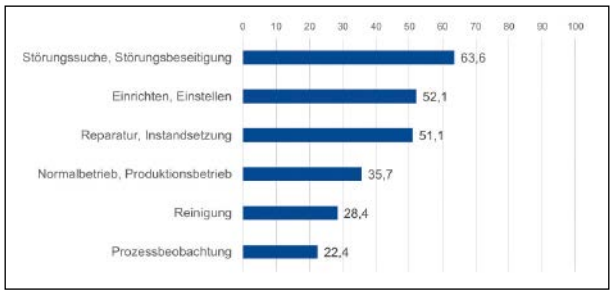
Ergebnis auf die Frage: „An wie viel Prozent der Maschinen wird Ihrer Einschätzung nach in Ihrem Betrieb/den von Ihnen betreuten Betrieben manipuliert?“



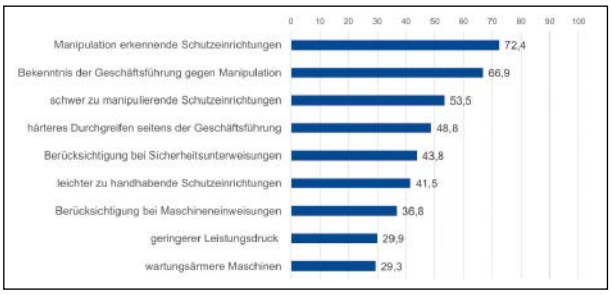
Ergebnis auf die Frage: „Gab es in Ihrem Betrieb/den von Ihnen betreuten Betrieben schon mal einen (Beinahe-) Unfall, dessen Ursache die Manipulation einer Schutzeinrichtung war?“ (Multiple Choice)



Ergebnis auf die Frage: „Falls Ihrer Erfahrung nach in Ihrem Betrieb/den von Ihnen betreuten Betrieben bereits eine Schutzeinrichtung manipuliert wurde: War dies einem Vorgesetzten bekannt?“



Ergebnis auf die Frage: „Für welche Arbeitsaufgabe werden Ihrer Erfahrung nach Schutzeinrichtungen am häufigsten manipuliert?“



Ergebnis auf die Frage: „Welche Maßnahmen tragen Ihrer Meinung nach besonders zur Verhinderung von Manipulation bei?“

Interview mit Stefan Otto

Stefan Otto, Prüfingenieur für Funktionale Sicherheit im Institut für Arbeitsschutz (IFA) und Leiter des Arbeitskreises Manipulation von Schutzeinrichtungen der Deutschen Gesetzlichen Unfallversicherung (DGUV)

GIT SICHERHEIT: Herr Otto, Manipulation ist wahrscheinlich ein häufig unterschätztes Thema im Bereich Maschinen- und Anlagensicherheit. Daher würde uns vor allem zunächst interessieren, wie genau es zu dieser Umfrage kam und auf welche Hürden Sie dabei gestoßen sind?

Stefan Otto: Dass Schutzeinrichtungen an Maschinen manipuliert werden, ist nicht neu. Eine 2004 durch das BGIA (heute IFA) und Berufsgenossenschaften der metallverarbeitenden Industrie durchgeführte Studie belegte, dass in den damaligen metallverarbeitenden Betrieben rund 37 % aller Schutzeinrichtungen manipuliert werden. Schätzungen von Arbeitsschutzexperten zufolge werden hierdurch rund ein Viertel aller jährlich stattfindenden Arbeitsunfälle an Maschinen verursacht. Die Zahlen stellten einen Weckruf an Arbeitsschützer dar, sich eingehender mit der Thematik zu befassen. Seither hat das Thema zunehmend Eingang in Richtlinien, Verordnungen und Normen gefunden. Trotz dieser Fortschritte geschehen jedoch immer wieder auf die Manipulation von Schutzeinrichtungen zurückzuführende Arbeitsunfälle, und betriebliche wie berufsgenossenschaftliche Sicherheitsexperten berichten von einem anhaltendem Manipulationsgeschehen.

Aus diesem Grund, und um die Befunde der zurückliegenden Manipulationsstudie auf den aktuellen Stand zu bringen, hat das IFA eine Umfrage durchgeführt. Als Zielgruppe der Umfrage wurden vorrangig solche Personen definiert, die mit der Arbeitssicherheit in Industrie- und Handwerksbetrieben vertraut sind, da hier von der größten Dichte an Maschinen auszugehen ist. Dabei wurde im Gegensatz zu der genannten Studie von 2004 explizit auf eine darüber hinausgehende Branchenzugehörigkeit der Betriebe verzichtet, um ein übergreifendes Bild des aktuellen Manipulationsgeschehens zu erhalten. Der Fragebogen selbst wurde mit insgesamt 16 Fragen und einer geschätzten Bearbeitungsdauer von unter fünf Minuten absichtlich niederschwellig ausgeführt, um eine möglichst große Teilnahmebereitschaft zu erzeugen. Dennoch wurden erst nach wiederholten Bemühungen durch Verteilung auf Veranstaltungen, in Print- und Online-Magazinen, Newslettern und auf Social Media eine repräsentative Anzahl von Rückläufern erzielt. Die Rückläufer selbst zeigten dann allerdings, welche Brisanz das Thema auch aktuell besitzt.

Dann kommen wir doch einmal direkt zu den Ergebnissen: Bei welchen Arbeitsaufgaben und bei welcher Art von Schutzeinrichtung kommt es laut der Umfrage denn am häufigsten zu Manipulationen? Und spielt die Unternehmensgröße dabei eine Rolle?

Stefan Otto: Wie zu erwarten war, stellen Aufgaben, die einen manuellen Eingriff in den Gefahrenbereich der Maschine erfordern, die Hauptursache für das Umgehen von Schutzeinrichtungen dar. Dies kann darauf hindeuten, dass die Maschinen über keine geeigneten Betriebsarten für solche Tätigkeiten verfügen oder die Schutzeinrichtungen die Durchführung der Tätigkeit erheblich behindern. Beispiele hierfür sind die Störungssuche, das Einrichten oder Tätigkeiten für die Instandhaltung von Maschinen. Manipuliert werden überwiegend abschrankende, trennende Schutzeinrichtungen wie Zäune oder Schutztüren, da diese

Bitte umblättern ▶

◀◀ zurück zum Inhaltsverzeichnis

im Arbeitsablauf am ehesten als Einschränkung wahrgenommen werden.

Was die Unternehmensgröße anbelangt, so schneiden kleinere Betriebe in der Umfrage tatsächlich schlechter ab als größere. Gemäß der Umfrage zeigen Kleinst- und Kleinbetriebe (1 bis 49 Beschäftigte) gegenüber Großbetrieben (ab 250 Beschäftigte)

- eine um 13,7 % erhöhte Manipulationshäufigkeit
- eine um 14,7 % erhöhte Duldung der Manipulation durch Vorgesetzte
- eine um 7,8 % verringerte Berücksichtigung des Themas in Schulungen und Unterweisungen
- eine um 31,2 % verringerte Berücksichtigung des Themas bei der Beschaffung von Maschinen

Gründe für diese Auffälligkeit sind neben einer flacheren Hierarchie und größeren Sichtbarkeit solcher Vorfälle sicher auch in den geringeren finanziellen wie personellen Ressourcen zu finden.

Welches Ergebnis hat Sie denn persönlich am meisten überrascht?

Stefan Otto: Zunächst muss die positive Tendenz der Zahlen hervorgehoben werden: So gaben 57,3 % der Befragten an, dass heute weniger Schutzeinrichtungen von Maschinen in Betrieben manipuliert werden als noch vor zehn Jahren. Dennoch ist der Anteil der ständig oder vorübergehend manipulierten Maschinen mit 27,2 % natürlich zu hoch. Das gleiche gilt für die damit einhergehende, mit nahezu 50 % erschreckend hohe Anzahl an Rückläufern, die von Unfällen oder Beinahe-Unfällen an manipulierten Maschinen berichten. Ebenfalls überrascht hat mich der rund 50-prozentige Anteil an Rückmeldungen, in denen die Befragten von der Kenntnis eines Vorgesetzten von einer durchgeführten Manipulation berichten.

Letzteres muss nicht notgedrungen als Hinweis darauf interpretiert werden, dass in solchen Betrieben Manipulationen an Maschinen oder Schutzeinrichtungen generell geduldet werden. Jedoch zeigt der Zusammenhang solcher Fälle – und seien es Einzelfälle – mit der einhergehenden Manipulationshäufigkeit in solchen Unternehmen den immensen Einfluss des Führungskräfteverhaltens auf die betriebliche Arbeitssicherheit. So zeigen Betriebe, in denen Manipulation – auch in Einzelfällen – von Führungskräften geduldet wird, gegenüber anderen Betrieben

- eine um 10,1 % erhöhte Manipulationshäufigkeit
- ein um 18 % erhöhtes Unfallgeschehen

Doch die Umfrage zeigt auch positive Tendenzen. So ist das Thema Manipulation in den meisten Betrieben mittlerweile fester Bestandteil in Schulungen und Unterweisungen und wird dort in 60 % der Fälle regelmäßig, in 30 % der Fälle zumindest selten aufgegriffen. Bei der Beschaffung von Maschinen wird das Thema in 56,7 % der Fälle mitberücksichtigt.

Wie beurteilen Sie die Ergebnisse? Was müsste sich z. B. ändern, um Manipulation weiter einzuschränken? Und gibt es diesbezüglich bereits Ansätze?

Stefan Otto: Die Ergebnisse der Umfrage zeigen, dass Präventionsarbeit auch an der in einem Betrieb gelebten Führungs- und Sicherheitskultur ansetzen muss. Die Sicherheit der Angestellten muss in Unternehmen immer an erster Stelle stehen. Dies kann nur geschehen, wenn dies auch von den Vorgesetzten im Unternehmen vorgelebt und propagiert wird. Sichere, in den Arbeitsablauf integrierte Schutzeinrichtungen leisten einen weiteren Beitrag.

Die Wichtigkeit der Führungskultur wird in auch in den Betrieben erkannt. Dies zeigen die Antworten auf die Frage, welche Maßnahmen besonders zur Verhinderung von Manipulation beitragen. Die dahinterliegende Sicherheitskultur rückt indes bereits seit einigen Jahren mit Präventionskampagnen wie Vision Zero immer mehr in den Fokus der berufsgenossenschaftlichen Präventionsarbeit. Gleichzeitig muss die Präventionsarbeit der Unfallversicherungsträger mehr darauf ausgerichtet werden, dass auch kleine Betriebe erreicht werden. Die Umfrage zeigt, dass hier Nachholbedarf besteht.

Weiterführende Hinweise:

https://stop-defeating.org

Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA)
Sankt Augustin
Tel.: +49 30 13001 0
ifa@dguv.de
https://www.dguv.de/ifa/stopp-manipulation

Effizientes Energiemanagement

Das Energiemeter RL 9405 von E. Dold dient zur Messung elektrischer Kennwerte und Energieverbräuche in 3-Phasen-Netzen mit Neutralleiter. Spannungen und Ströme werden kontinuierlich gemessen und ausgewertet. Eine separate Hilfsspannung ist nicht erforderlich. Das Gerät liefert bis zu 50 Kenngrößen der Energieversorgung und das bei einer kompakten Baubreite von nur 35 mm. Das RL 9405 ermittelt alle Energieverbräuche und ermöglicht die Aufschlüsselung nach Verursachung. Das Energiemeter ist prädestiniert unter anderem für den Einsatz in Fertigungsprozessen und IT-Rechenzentren, um Energieeinsparpotenziale aufzudecken, und eignet sich vor allem auch für die Erfüllung von Energieaudits (DIN EN 16247-1) bzw. Energiemanagement (ISO 50001).

© E. Dold

www.dold.com

Funk-Sicherheitsmodul UH 6900

Mit dem Funk-Sicherheitsmodul UH 6900 ergänzt Dold seine Kompetenzen im Bereich der drahtlosen funktionalen Sicherheit. Neben dem sicheren Funk-Not-Halt-System sowie dem kabellosen Zustimmtaster der Safemaster-W-Familie bietet das Unternehmen eine sichere, bidirektionale Sicherheitslösung, die in verschiedenen Applikationen kabellos integriert werden kann. Selbst in Bereichen, in der klassische Sicherheitstechnik an Grenzen stößt, können nun per Funk Signale sicher übertragen werden. Das Wireless-Safety-System der Safemaster-W-Familie ermöglicht eine sichere Bedienung und Abschaltung von Anlagen mit Gefahrenzonen, wie etwa im Automatikbetrieb (z. B. Störungsbeseitigung, Schmierdienst, Justagearbeiten) oder im Einrichtbetrieb (z. B. Inbetriebnahmen, Maschineneinstellungen, Wartungen).


© E. Dold

www.dold.com

◄◄ zurück zum Inhaltsverzeichnis

GIT SICHERHEIT

INNENTITEL – ARBEITSSCHUTZ

GEFAHRSTOFFLAGERUNG

IoT-Leckage-Warnsystem entlastet Betreiber von Auffangwannen

Spillguard Connect-Sensor mit DIBt-Zulassung erfüllt Prüfpflichten

Die Firma Denios SE aus Bad Oeynhausen hat mit der kürzlich erworbenen DIBt-Zulassung für das IoT-Leckage-Warnsystem SpillGuard connect einen wichtigen Durchbruch erzielt. Betreiber von Auffangwannen sind gesetzlich nach dem Wasserhaushaltsgesetz (WHG) dazu verpflichtet, eine wöchentliche Sichtprüfung durchzuführen, um mögliche Leckagen zu erkennen und zu beseitigen. Diese Sichtprüfung kann nun entfallen, wenn das IoT-Leckage-Warnsystem SpillGuard connect zum Einsatz kommt. Das gerade mal handgroße, autark betriebene Gerät spart produzierenden Unternehmen wertvolle Arbeitszeit und erhöht zusätzlich die Sicherheit im Betrieb.

◀◀ zurück zum Inhaltsverzeichnis

Beim SpillGuard connect handelt es sich um ein innovatives Warnsystem im Bereich der Gefahrstofflagerung: Das Gerät ist mit Batterie und Mobilfunk ausgestattet und mit nur einem Knopfdruck autark funktionsfähig. Es detektiert jede Art von Flüssigkeiten. Sollte es nun zu einer Leckage kommen, erkennt der SpillGuard connect dank des eingebauten Sensors diese Gefahrensituation und schlägt Alarm – per Blinken und Piepton macht das Gerät auf sich aufmerksam. Gleichzeitig wird per E-Mail oder SMS über den Vorfall informiert, so dass eine schnelle Reaktion erfolgen kann. Dadurch werden effektiv Unfallrisiken, Folgekosten sowie rechtliche Konsequenzen minimiert.

Zeitraubende Sichtprüfungen entfallen

Bislang mussten Unternehmen ihren wöchentlichen Betreiberpflichten nachkommen, indem sie regelmäßig und mühsam alle Auffangwannen im Betrieb einer Sichtkontrolle unterzogen, ob sich darin Flüssigkeiten befinden. Eine Prozedur, die viel Zeit in Anspruch genommen hat: Ein Unternehmen mit beispielsweise 20 Auffangwannen hat bislang mehrere Stunden pro Woche dafür benötigt, um den vorgeschriebenen Kontrollgang zu absolvieren. Rechnet man diese Arbeitszeit auf ein ganzes Jahr hoch, so hat dieses Unternehmen mehr als sieben Arbeitstage mit der Sichtkontrolle der Auffangwannen verbracht. Wertvolle Arbeitszeit, die nun dank des SpillGuard connect mit DIBt-Zulassung sinnvoller eingesetzt werden kann. Das Reporting erfolgt ebenfalls einfach per Knopfdruck. Auch wenn kein Leckage-Ereignis eintritt, speichert der SpillGuard connect einmal wöchentlich den Status und belegt so im Reporting in Kombination mit der DIBt-Zulassung die Erfüllung der betreiberseitigen Prüfpflichten.

Keine Leckage bleibt mehr unerkannt

Dass flüssige Gefahrstoffe auslaufen, kann jederzeit passieren. Wer das Gebinde auf einer Auffangwanne lagert, hat erst einmal alles richtig gemacht: Sie verhindert zuverlässig, dass die gefährlichen Stoffe ins Erdreich gelangen. Häufig werden ausgelaufene Flüssigkeiten in der Auffangwanne aber nicht sofort entdeckt – zum Beispiel, wenn nicht ständig Personal anwesend ist. Eine nicht bereinigte Leckage kann jedoch schnell gefährlich werden. Bei besonders heiklen Stoffen, die etwa gefährliche Dämpfe absondern, ist schnelles Handeln gefragt. Außerdem muss die Funktionsfähigkeit der Auffangwanne – und damit auch das gesetzlich vorgeschriebene Auffangvolumen – zu jeder Zeit gegeben sein. Wenn sich bereits Flüssigkeit in der Wanne befindet, ist dies womöglich nicht mehr gewährleistet. Das IoT-Leckage-Warnsystem Spillguard connect detektiert rund um die Uhr auslaufende Flüssigkeiten und meldet Leckagen sofort – auch wenn kein Mensch in der Nähe ist. Eine Statushistorie sorgt für die Nachvollziehbarkeit von Meldungen.

Datenübertragung per Narrowband IoT

Die Anbindung der Leckage-Überwachung an ein Mobilfunknetz ermöglicht einen vom Firmennetzwerk unabhängigen Zugriff auf die Daten und Alarmmeldungen. NarrowBand IoT ist eine sichere und effiziente Mobilfunk-Netztechnologie für diese Anwendung. Dieser weltweite Industriestandard basiert auf LTE und nutzt die zugehörigen Sicherheitsmechanismen nach 3GPP. Da die Technologie speziell auf kleinere Datenmengen ausgerichtet ist, bietet sie eine besonders kosteneffiziente und zuverlässige Mobilfunk-Kommunikation.

Per NarrowBand IoT werden sicher und effizient Alarmmeldungen und das Reporting auf die App der Nutzer weitergeleitet

Sicherheit mit Brief und Siegel

Bei der DIBt-Zulassung für SpillGuard connect handelt es sich um eine allgemeine bauaufsichtliche Zulassung (abZ). Mit dieser können regelungsbedürftige Bauprodukte und konstruktive Lösungen deutschlandweit in Einklang mit den Bauordnungen ver- und angewendet werden. Für den Erwerb der DIBt-Zulassung wurde das IoT-Leckage-Warnsystem umfangreichen Prüfungen unterzogen. Im Fokus standen neben Hard- und Softwaretests aufwendige Prozessnachweise insbesondere für IoT-Tauglichkeit und Medienbeständigkeit (Dämpfe und Flüssigkeiten). Neben der Bauprodukte-Zulassung (abZ) verfügt der SpillGuard connct über eine Zulassung nach ATEX-Richtlinie 2014/34/EU und Funkzulassung nach RED Richtlinie 2014/53/EU.

Um den SpillGuard connect gesetzeskonform zu betreiben müssen bei Stahlwannen die Vorgaben der StawaR beachtet werden. Generell ist das Gerät gemäß der Herstellervorgaben in der Wanne zu positionieren. Danach ist eine einmalige Sicherstellung der Funkverbindung erforderlich. Die erstmalige Verbindungsprüfung erfolgt im Rahmen der Registrierung in der Web-Applikation. Eine wöchentliche Verbindungsprüfung sorgt für eine Fehlermeldung, wenn die Verbindung gestört ist.

Registrierung und initiale Konfiguration der Web-Applikation übernimmt das Denios Service Team. Sobald der Kunden-Account in der Web-Applikation aktiviert wurde, können Betreiber ihre Geräte direkt einsehen und Benachrichtigungen individuell verwalten. Der SpillGuard connect kann nach einmaliger Aktivierung in der Web-Applikation vollumfänglich genutzt werden.

Der Leckagesensor verfügt zudem über die Ex-Schutzklasse Ex II 1G Ex ia ma IIB T4 Ga und ist für Ex-Zone 0 zugelassen. Vor

SpillGuard connect detektiert zuverlässig jede Form von Leckage. Dank der DIBt-Zulassung sparen Unternehmen zudem wertvolle Arbeitszeit, durch den Wegfall der bisher nötigen Kontrollgänge

Bitte umblättern ▶

◀◀ zurück zum Inhaltsverzeichnis

dem Einsatz des Gerätes in einer Ex-Zone ist vom Betreiber im Rahmen der Gefährdungsbeurteilung zu bewerten, ob und wo das Gerät eingesetzt werden darf.

Branchenübergreifend und in vielen Anwendungen einsetzbar

SpillGuard connect ist hersteller- und ortsunabhängig, so dass beliebige Auffangwannen und Lager damit ausgestattet werden können. Die Medienbeständigkeit ist für den Einsatz mit allen gängigen flüssigen Gefahrstoffen gegeben. Über den QR-Code am Ende dieses Beitrags ist eine Beständigkeitsliste abrufbar, die angibt, für welche Gefahrstoffe die Funktionalität des SpillGuard connect über den definierten Zeitraum von mindestens 24 Stunden nachgewiesen wurde. Für einen in der Beständigkeitsliste nicht aufgeführten Stoff kann auf Wunsch ein Labortest durchgeführt werden, der die Eignung des SpillGuard connect überprüft. Einsetzbar ist das neuartige Leckage-Warnsystem nicht nur in Lagerräumen, sondern überall dort, wo Gefahrstoff-Leckagen detektiert werden sollen, wie Pumpensümpfe, Prüfstände, Rohrleitungen,

Der handgroße SpillGuard Connect ist mit nur einem Knopfdruck autark funktionsfähig und bietet über 5 Jahre-Laufzeit ein umfassendes Condition Monitoring

Labore, in Werkhallen oder anderen z. T. schlecht zugänglichen oder Ex-Schutzzonen.

Die Anschaffungskosten sind schnell amortisiert

Bereits nach ca. 5 eingesparten Arbeitsstunden haben sich die Anschaffungskosten amortisiert. Der Sicherheitsgewinn kommt noch hinzu. Mobilfunk und Cloud-Services sind für die Dauer von 5 Jahren bereits inbegriffen, denn bis zu 5 Jahre Laufzeit bietet die Batterie. Diese kann aufgrund der ATEX-Schutzvorkehrung nicht ausgetauscht werden.

Durch die aktuell erteilte Zulassung vom „Deutschen Institut für Bautechnik“ entwickelt sich das IoT-Warnsystem SpillGuard connect der Denios SE zu einem unverzichtbaren Rund-um-die-Uhr-Wächter für alle, die mit dem Thema Gefahrstofflagerung zu tun haben. ●

Weitere Informationen zur Beständigkeitsliste:

https://www.denios.de/unternehmen/marken/spillguard

Denios SE
Bad Oeynhausen
Tel.: +49 5732 753 0
info@denios.de
www.denios.de

„Dreifach grüner“ Arbeitsschuh

„Dreifach grüner“ Sicherheitsschuh von Atlas

Der Atlas Recycling Safety Shoe besteht nicht nur aus recycelten Materialien. Jeder Part des Schuhs wurde ganzheitlich und nachhaltig durchdacht. Obermaterial, Zwischensohle und Einlegesohle bestehen aus innovativen Materialien und nutzen intelligente Prozesse in der Produktion zur effizienteren Rohstoffverwertung. Das Ergebnis: ein dreifach grüner Sicherheitsschuh – Nachhaltigkeit zum Anfassen.

Aus Mesh-Obermaterial wird PET-Obermaterial: Der Schaft des Recycling Safety Shoe besteht zu 92 % aus wiederverwerteten PET-Flaschen. Dafür verwendet der Hersteller einen speziellen Polyester namens Repreve, den schon zahlreiche namhafte Brands nutzen. Um Repreve Polyester herzustellen, werden weltweit gesammelte Kunststoffflaschen und postindustrielle Abfälle zerkleinert, gemahlen, gewaschen und zu hochwertigen Spänen verarbeitet. Diese Späne werden zu flüssigem Polymer geschmolzen und durch winzige Öffnungen in einer Spinndüse extrudiert, wobei Filamente entstehen, die die Repreve-Faser bilden. Das Unternehmen Unifii spinnt die Faser zu Garn, aus dem ein Stoff gewoben wird: der Repreve-Polyester. Das zu 100 % gewebte und nahtlose Obermaterial kombiniert Halt und Performance mit angenehm weichem, elastischem Komfort für ein natürliches Laufgefühl – und das mit gutem Gewissen. In einem umfassenden Prozess wurde der Hersteller mit dem U-Trust-Zertifikat ausgezeichnet, das die Einhaltung der Repreve Certification Standards beim Recycling Safety Shoe bestätigt.

Die Sohle besteht aus hauseigenem MPU (Multifunktionales Polyurethan). Bei der Herstellung der Zwischensohle in der Direktbesohlungsanlage entstehen natürlicherweise Produktionsabfälle. Diese PU-Reste fängt das Unternehmen auf, granuliert sie mit dem eigenen MPU-Cutter und führt sie wieder dem Produktionskreislauf zu. 20 % der Zwischensohle des Recycling Safety Shoe bestehen aufgrund dieses Prozesses aus zudosierten Feststoffen. Bei der Zwischensohlenherstellung eines einzelnen Schuhs kann der Hersteller also ein Fünftel an Primärmaterialien einsparen und so den Rohstoffeinsatz (Polyol und Isocyanat) reduzieren. Das MPU-Rebound-System federt effektiv und sofort nach dem Auftreten in seine Ursprungsform zurück. Somit hat der Träger eine optimale Kraftverteilung und die Gelenke werden entlastet.

Der Recycling Safety Shoe kommt zusammen mit der Recycling Insole Climate Comfort. Die Recycling Insole Clima Comfort besteht aus 86 % recyceltem Ecofoam. Die Zusammensetzung des Ecofoams basiert auf der vollständigen Wiederverwendung aller Abfälle, einschließlich derjenigen, die bei der Herstellung von Einlegesohlen anfallen. Die Sohle ist besonders atmungsaktiv, schnell trocknend und gewährleistet eine optimale Auftrittsdämpfung im Vorderfußbereich sowie durch den verstärkten Fersenpunkt.

www.atlasschuhe.de

◄◄ zurück zum Inhaltsverzeichnis

WALK ON THE SAFE SIDE

ELTEN.COM

WELLNESS FÜR DIE FÜSSE

ELTEN

BENTE XXE GTX GREEN MID ESD
BENTE XXE GTX BLUE LOW ESD

ART.-NR.: 760731 + 720721 | GR: 40 – 48

ERREICHT EIN NEUES DÄMPFUNGSLEVEL DURCH DEN SOHLENKERN AUS INFINERGY® VON BASF.

SICHERHEITSKLASSE S3

WELLMAXX

Infinergy®

Made with Infinergy® by BASF

Deutsche Standards
MARKE DES JAHRHUNDERTS 2022

MULTINORM-PRODUKTVERGLEICH

Nicht Jacke wie Hose

Multinorm-Schutzkleidung in der Übersicht

Aufgabe der Multinorm-Schutzkleidung ist es, Gefährdungsprofile umfassend abzudecken. Die folgende Zusammenstellung bietet eine vergleichende Übersicht zu Multinorm-Schutzkleidung von fünf Herstellern bzw. Leasinganbietern und geht zugleich der Frage nach, wann die Anschaffung zwingend erforderlich bzw. sinnvoll ist.

Welche potenziellen Gefahren von einer Arbeitsstätte als Ganzes, aber auch von jedem einzelnen Arbeitsplatz ausgehen, wird im Rahmen der Gefährdungsbeurteilung analysiert und festgehalten. Sie ist damit die Basis für alle Maßnahmen zum Arbeits- und Gesundheitsschutz, die der Arbeitgeber für ein sicheres Arbeitsumfeld seiner Mitarbeiter umsetzen muss. Aus den benannten Risiken sind die Schutzfunktionen der Schutzkleidung und die Notwendigkeit weiterer Schutzausrüstung abzuleiten.

	DBL	Fristads
Produktname	Comfort Color Multiprotect Bundjacke Comfort Color Multiprotect Bundhose	Flamestat High Vis Airtech Jacke KL.3 4525 ATHR Flamestat High Vis Airtech Hose KL.2 2525 ATHR
Abgedeckte Normen	• EN 1149-5: Schutz vor elektrostatischer Aufladung • EN 11612 A1 + A2 B1 C1 E2 F1: Schutz gegen Hitze und Flammen • EN 13034+A1 Typ 6: Schutz vor Chemikalien • EN ISO 11611 Klasse 1 A1 + A2: Schweißerschutz • IEC 61482-2_ 2018 APC 1: Schutz vor Störlichtbögen	• EN 343 Regenschutz • EN ISO 11611 Schweißer-Schutz • EN 13034 Schutz (begrentzt) vor flüssigen Chemikalien • EN ISO 11612 Schutz vor Hitze und Flammen • EN 1149 Schutz vor elektrostatischer Entladung • EN 14404 Knieschutz • EN 20471 Warnschutz • IEC 61482-2 Störlichtbogen, mit ELIM-Wert
verfügbare Größen	Jacken 40/42 – 64/66, 90/94-114/118 Hosen 23-30, 42-68, 94-114	XS-3XL
Gewicht	300 g/m²	Außenmaterial 260 g/m². Futter 130 g/m²
Listenpreis (Netto)	Leasing	Jacke: 494,90 € Hose: 450,90 €
Einsatzbereiche	• Energieversorger • Schweißarbeiten • Chemische Industrie • Handwerk • Petrochemie	• Energieversorger • Verkehrs- und Baubetriebe • Kommunen
Eigenschaften	• hoher Tragekomfort • leichte Grammaturen • modern und ergonomisch geschnitten • mit Stretchanteil	• Wasserdicht, • Winddicht • Atmungsaktiv • Inhärenter Flammschutz
Verwendete Materialien	75% Baumwolle, 24% Polyester, 1% Carbon	Wasserdichtes, winddichtes und atmungsaktives Airtech-Material. 50% Modacryl, 41% Baumwolle, 7% PU, 2% antistatische Faser, 2-Lagen-Laminat. Verschweißte Nähte; Futter 50% Aramid, 50% Viskose FR; Inhärenter Flammschutz
Besonderheiten	Multiple Schutzfunktionen kombiniert mit leichten Grammaturen, dadurch angenehm zu tragen, was auch durch die moderne, ergonomische Schnittführung zu hoher Akzeptanz führt, so dass auch Schutzkleidung gerne getragen wird.	Günstigere Alternative zu Gore Tex durch die selbstentwickelte Airtech Membran. Deutlicher Preisunterschied und daher interessant für große Projekte.

Erfüllt die Schutzkleidung, abgesehen von der EN ISO 13688, mehr als eine Norm, spricht man von Multinorm-Schutzbekleidung. In diese Kategorie fällt zum Beispiel die Schutzkleidung für Schweißen und verwandte Verfahren. Neben der eigentlichen Schweißerschutznorm EN ISO 11611 muss sie auch der EN ISO 11612 „Schutzkleidung gegen Hitze und Flammen" entsprechen.

Weitere typische Einsatzbereiche für Multinorm-Schutzkleidung sind bei Energieversorgern, Entsorgungs- und Industriewartungsunternehmen, Raffinerien und Gefahrguttransporteuren. In diesen Branchen reichen Hitze- und Flammschutz oftmals nicht aus. Je nach Arbeitsumgebung und Tätigkeit besteht zusätzlich die Gefahr der Einwirkung eines Störlichtbogens und/oder einer elektrostatischen Aufladung mit dem Risiko der Explosion von Gas- und Staubgemischen.

So müssen Fachmonteure im Umgang mit Schaltanlagen oder beim Kabelverbau Multinorm-Kleidung tragen, die neben der EN ISO 11612 auch die IEC 61482-1-2 „Schutz gegen thermische Gefahren eines Störlichtbogens" und die EN 1149-5 „Elektrostatische Eigenschaften" erfüllt. Wer beispielsweise bei Wartungs- und Transporttätigkeiten mit Kraftstoffresten bzw. explosiven Rückständen in Berührung kommen kann, benötigt Schutzkleidung sowohl mit flammhemmenden als auch mit antistatischen Eigenschaften.

Vergleichsweise neue Anforderungen resultieren in der Automobilfertigung aus dem Verbau von Hochvoltbatterien – oder für Arbeiten bei unklarer Lage an nicht fahrtüchtigen Hybridfahrzeugen. Hier gilt es, die speziell geschulten Mitarbeiter außer gegen Funkenflug und die thermischen Gefahren eines Störlichtbogens auch gegen Gefährdungen durch Hitze und Flammen zu schützen. Wo viel Fahrverkehr herrscht, kommt der Warnschutz (EN ISO 20471) und im Außenbereich der Wetterschutz (EN 343) als weitere Anforderung hinzu.

HB	Helly Hansen Workwear	Kübler
HB-MultiPro FR Parka 7kA HB-MultiPro FR Latzhose 7kA	Fyre Jacket (77249) Fyre Construction Pant Class 2 (77452)	Kübler Protectiq Jacke | Form 1391 Kübler Protectiq Hose | Form 2391
• EN ISO 20471 Klasse 3 – Warnschutz • EN 343 Klasse 3/3 – Wetterschutz • IEC 61482-2 Klasse 2 – Störlichtbogenschutz • EN ISO 11612 A1/B1/C1/E1/F1 – Schutz gegen den Kontakt mit Flammen, Strahlungshitze, Kontakthitze, Konvektive Hitze und flüssige Eisenspritzer • EN ISO 11611 Klasse 2 A1 – Schweißerschutz • EN 1149-5 – antistatische Eigenschaften • EN 13034 Typ PB [6] – Schutz vor Chemikalien	• EN ISO 20471:2013 klasse 2 (hochsichtbare Warnbekleidung) • IEC 61482-2:2018 APC 1, EBT 9 cal/cm² in Kombination mit 77449, 77450, 77451, 77452, 77249 (Schutz vor thermischen Gefahren durch Lichtbogen) • EN 11612:2015 A1 B1 C1 D2 E2 F1 (Jacke) und EN 11612:2015 A1 B1 C1 F1 (Hose) (Schutz vor Hitze und Flammen) • EN 11611:2015 klasse 1, A1 (Schutz bei Schweißverfahren) • EN 1149-5:2018! (Schutz vor elektrostatischen Entladungen)	• EN ISO 11611, Klasse 1-A1 • EN ISO 11612, Code A1 B1 C1 D1 E2 F1 • IEC 61482-2 APC=2 • EN 1149-5 • EN 13034 + A1:2009 Typ 6 • ELIM-Wert: 16 cal/cm² • EN ISO 15797
38/40 bis 70/72	Jacken XS – 4XL Hosen C44-C48, D88-D124	44-64, 90-114, 24-30
ca. 320 g/m²	310 g/m²	ca. 320 g/m²
auf Nachfrage	auf Nachfrage	Jacke: 335,60 € Hose: 282,75 €
• Energieversorger und Stadtwerke • Verkehrs- und Baubetriebe, • Logistik, Schienen- und Gleisbau • Petrochemie • Fahrleitungs- und Anlagenbau • Netztechnik und Schaltanlagen • Abfallwirtschaft und Entsorgung	• Metallindustrie • Verkehrs- und Baubetriebe • Schweißarbeiten	• Energieversorger • Raffinerien • Tanklager • Chemische Industrie • Abfallwirtschaft • Stadtwerke
• Wind- und wasserabweisend • Atmungsaktiv • Strapazierfähig • Auch für Herbst und Winter geeignet	• Hitze- und flammenbeständig • Elektrostatische Eigenschaften • Hohe Sichtbarkeit	• Industriewäsche geeignet nach EN ISO 15797 • Zahlreiche Taschenlösungen • Ergonomisch geschnittene Ärmel • Reflexelemente
48% Modacryl, 32% Baumwolle, 18% Polyester, 2% Carbon; mit Futterliner	Jacke und Hose bestehen jeweils aus OEKO-TEX® zertifiziertem 45% Modacryl und 33% Baumwolle, 18% Polyamid und 3% Elastan – 1% machen sonstige Fasern aus. Ein äußerst strapazierfähiges und gleichzeitig komfortables Workwear-Outfit.	Oberstoff aus 47% Modacryl, 32% Baumwolle, 20% Polyamid und 1% antistatische Faser
Sehr hochwertige Materialien, verschweißte Nähte, eingearbeitete Membran, 2-Wege-Reißverschluss, Rückenverlängerung, zusätzliche Fleecejacke zum einhängen, zusätzliche Kapuze zum anknöpfen, verstellbare Taillen- und Saumweite, flammhemmendes Obermaterial, industriewaschtauglich.	Die Jacke verfügt über einen Haken für die Befestigung eines Funkgeräts, eine praktische Napoleontasche sowie eine Schlaufe für einen Ausweis oder ID-Karten. Die Hose verfügt über Kniepolstertaschen sowie eine optionale Beinverlängerung um 5 cm.	Auch als Warnschutz-Variante und separater Schweißerschutzvariante verfügbar – inklusive Wetterprodukte.

SICHERHEITSHANDSCHUHE & -SCHUHE

Das hat Hand und Fuß

Spezielle Arbeitsbereiche erfordern spezielle PSA-Lösungen

Die Arbeitsplatzbedingungen sind nicht nur von Branche zu Branche unterschiedlich, auch innerhalb eines Unternehmens variieren diese je nach Umgebung und Tätigkeit mitunter sehr stark. Die passende PSA für den jeweiligen Bereich zu ermitteln, stellt vor diesem Hintergrund eine große Herausforderung dar. Um Produkte mit der höchstmöglichen Effizienz passend zu den jeweiligen Anforderungen auswählen zu können, sind umfangreiche Tests vor Ort daher unerlässlich. So auch bei der Weiss Spindeltechnologie GmbH, die der PSA-Spezialist Ejendals seit 2019 sowohl mit Handschuhen als auch Sicherheitsschuhen ausstattet.

Das mittelständische Produktionsunternehmen hat sich als Entwickler und Produzent von hochpräzisen Spindeleinheiten in der Branche einen Namen gemacht. Gefertigt werden Motorspindeln für Fräs-, Dreh- und Schleifbearbeitungszentren, aber auch Sonderspindeln, die zum Beispiel in der Milchpulverindustrie oder in Entschwefelungsanlagen in Müllkraftwerken eingesetzt werden. Das Unternehmen liefert ein komplettes Spektrum an standardisierten sowie individuellen Lösungen und realisiert deren Einbettung in mechatronische Gesamtsysteme.

Persönlicher Arbeitsschutz ist in folgenden Bereichen relevant: in der Vorfertigung (hierzu zählt der Wareneingang und die Prüfung), beim Entgraten, beim Waschen und Verpacken sowie in der Schleiferei, dem Schrumpfen, der Montage, der Endprüfung und beim Warenausgang.

Funktionalität und Tragekomfort

Im Laufe der Erstanalyse nimmt das Ejendals-Team die Arbeitsplatzsituation seiner Kunden genau unter die Lupe. Dabei gilt es abzuklären, welche Bedingungen im jeweiligen Tätigkeitsbereich herrschen und wie die einzelnen Arbeitsschritte konkret aussehen. Darüber hinaus ist relevant, mit welchen Materialien die Mitarbeiter arbeiten.

„Ein Sicherheitsprodukt für alle Fälle gibt es nicht“, erklärt Jens Richkaus, Key Account Manager bei Ejendals. „Aktuell haben wir circa 343 unterschiedliche Handschuh- und circa 164 Sicherheitsschuh-Modelle im Sortiment. Und jeder einzelne Artikel hat seine Berechtigung.“ Denn selbst kleine Variationen in der Funktionalität und der Kombination unterschiedlicher Schutzanforderungen können ausschlaggebend sein, dass die PSA zur jeweiligen Arbeitssituation und Tätigkeit passt.

Für die Arbeitsplatzanalyse und umfangreiche Tragetests bei der Weiss Spindeltechnologie GmbH wählte Ejendals gemeinsam mit seinem Kunden mehrere Abteilungen am Produktionsstandort im bayerischen Maroldsweisach aus. Die Handschuhe wurden in zehn Bereichen, zum Beispiel in der Montage, Demontage und der Vorfertigung eingehend geprüft; die Schuhe vor allem in der Montage und der Schleiferei.

Individuelle Lösungen sind gefragt

Im Warenbereich herrschen stark schwankende Temperaturen. Darüber hinaus führen Nässe und Feuchtigkeit zu rutschigen Böden. Die Schuhe, die hier getragen werden, müssen vor allem einen guten Grip gewährleisten und auch Temperaturschwankungen ausgleichen können. Für den Handschutz liegt der Fokus insbesondere auf Griffsicherheit, denn die Mitarbeiter arbeiten hier mit verschiedenen Materialien. Ein weiterer Bereich, der spezielle Anforderungen an die PSA stellt, ist das Waschen/Entgraten und Verpacken. „Hier wird vorwiegend mit wässrigen Lösungen gearbeitet“, verdeutlicht Volker Sauerteig, bei Weiss Spindeltechnologie zuständig für den Arbeitsschutz. „Teile werden nach dem Vorfertigungsvorgang durch Schleifen entgratet und am Ende erfolgt noch ein Verpackungsvorgang.“ Somit sind hier die Ejendals Handschuhe gefragt, die sowohl in Bezug auf Schnittschutz als auch Griffsicherheit Höchstleistungen bringen. Die Sicherheitsschuhe müssen hingegen einen sehr guten Durchtrittschutz und dem Träger sicheren Stand auch auf rutschigem Untergrund gewähren.

▲ **Präzisionsarbeit bei der Beschriftung der Kühlbüchse zur Produktnachverfolgbarkeit ist gefragt. Im Einsatz: Tegera 113. Fingerspitzengefühl, Komfort und guter Schutz bei jedem Handgriff**

◄◄ zurück zum Inhaltsverzeichnis

Lösungen für problematische Bereiche

„Aufgrund unserer langjährigen Erfahrung, die wir mit den Kunden gesammelt haben, können wir relativ schnell die passenden PSA-Produkte für die jeweilige Tätigkeit empfehlen“, so Rickhaus „Darüber gibt es natürlich auch Abteilungen, die individuelle Lösungen und damit einhergehend eine umfassendere Beratung erfordern.“ Bei Weiss Spindeltechnologie war dies im Bereich „Schrumpfen“ der Fall. Hier stellt die Durchdringung von Wärme bei unterschiedlichen Temperaturen ein erhöhtes Sicherheitsrisiko dar. „Wir hatten 15 Jahr nach einer passenden Lösung gesucht, aber kein PSA-Anbieter konnte uns den idealen Handschuh anbieten“, erinnert sich Sauerteig. Mit dem Tegera 987 fand Ejendals schließlich den geeigneten Schutzhandschuh, der allen Anforderungen gerecht wird. Ein weiterer Spezialbereich: Als einziger Anbieter weltweit stellt Weiss Einzelteile (Kufen mit Zubehör) für die sogenannte Hydrostatik sowie Hydrodynamikspindeln her. Das mittelständische Unternehmen baut und repariert diese Art von Spindeln. „Hier geht es bei der Montage um den Gefahrstoff Öl“, verdeutlicht der Verantwortliche für Arbeitsschutz. „Die Mitarbeiter brauchen die Handschuhe zum Schutz vor diesem Gefahrstoff, müssen aber gleichzeitig das nötige Feingefühl behalten, um filigrane Montagetätigkeiten durchführen zu können.“ Der schwedische PSA-Spezialist hatte mit dem Tegera 7361 auch hier die passende Lösung parat.

Tragekomfort entscheidend

Wie der Arbeitsschutzverantwortliche verdeutlicht, lag dem Unternehmen die persönliche Einschätzung der Mitarbeiter sehr am Herzen. „Der Sicherheitsschuh ist der am längsten getragene Schuh des Tages“, verdeutlicht Sauerteig. „Daher sollte er sicherheitstechnisch in jeder Situation greifen und den Mitarbeiter beim Tragen der PSA das Gefühl von Bequemlichkeit, Tragekomfort und Zufriedenheit vermitteln.“ Aus diesem Grund wurde bei der Bedarfsanalyse dem Tragekomfort der Persönlichen Schutzausrüstung eine ebenso hohe Bedeutung beigemessen wie deren Funktionalität. Da der schwedische Markenhersteller kontinuierlich in neue Technologien investiert, damit seine Produkte ein Höchstmaß an Tragekomfort erzielen, hielten die getesteten Modelle dem kritischen Urteil der Belegschaft erfolgreich stand.

> „Wir suchten einen Problemlöser und fanden ihn!“

Fortsetzung folgt

Insgesamt 170 Angestellte und Azubis wurden in unterschiedlichen Abteilungen mit Hand- und Fußschutzprodukten von Ejendals ausgestattet. So sind beispielsweise Sicherheitsschuh-Modelle der Serien Zenit Evo im Einsatz. Ein Damen-Model der „Tempus-Serie“ soll folgen. Darüber hinaus wurden die Handschuhpläne auf den Weg gebracht.

„Wir suchten einen Problemlöser und fanden ihn“, verdeutlicht Sauerteig die gute Zusammenarbeit mit Ejendals und unterstreicht: „Hier stimmt einfach die Betreuung. Die Berater haben ein offenes Ohr für unsere Probleme und Nöte bei bestimmten Herausforderungen und finden in Problemsituationen schnell kompetente Lösungen und Methoden.“

Dank dieser vertrauensvollen Kooperation mit dem schwedischen PSA-Spezialisten in Kombination mit einem umfangreichen Arbeitsschutzprogramm inklusive regelmäßiger Besprechungen und Schulungen verzeichnet die Weiss Spindelkopftechnologie GmbH seit 1.680 Tagen keinen meldepflichtigen Unfall. ●

Ejendals
Leksand, Schweden
Tel.: +49 800 72 44 955
info@ejendals.com
www.ejendals.com

Ansprechpartner für Medien:
Regina Iglauer-Sander
info@coaching-communication.org

Einsatz an der Drehspindel im Schrumpfbereich. Bestens geschützt mir den Handschuhen Tegera 987 und Tegera 113. Für guten Gripp sorgen die sportlichen Zenit Evo 7138 Schuhe ▼

Andreas Wolf, Hydromonteur, an der Hydrostatikspindel. Die Hände werden durch den Tegera 777 geschützt im Einsatzbereich Hydromontage und Kufenfertigung ▼

SICHERHEITSSCHUHE

Hammerhartes Equipment mit dem Plus

Wie der Haix Connexis Safety+ für mehr Sicherheit und Tragekomfort in der Schmiede sorgt

Senior-Schmied Josef Kindermann bearbeitet sein Werkstück mit der Flex, um anschließend mit der Stahlbürste die Politur zu vollenden. Vor Funkenflug schützt dabei auch der neue Haix Connexis Safety+

Eine „Waidlapfanne“ ist ein hartes Stück Arbeit. „So sieht das aus, bevor wir anfangen“, sagt Stefan Kindermann und zeigt auf einen Eisenriegel von der Größe einer Tafel Blockschokolade. „Robustes Industrieeisen“, fügt der junge Schmied an. Bevor daraus allerdings eine von Hand geschmiedete Bratpfanne wird, muss das Metall erst einmal auf „Betriebstemperatur“ gebracht werden: Bei mindestens 1.000 Grad beginnt die Hammerarbeit, die höchste Konzentration erfordert und gutes Werkzeug. Komfortable Arbeitsschuhe sind dabei mehr als nur Schutz für die Füße. Der Haix Connexis Safety+ ist der robuste Sicherheitsschuh mit dem echten Plus, den Haix genau für solche Einsätze und solche Berufsfelder entwickelt hat: Ein Sicherheitsklasse-S3-Schuh mit der integrierten Faszien-Technologie von Haix, die aktiv die Faszien stimuliert und so Muskulatur und Blutfluss anregt und vorzeitigem Ermüden vorbeugt.

◀◀ zurück zum Inhaltsverzeichnis

Die schwere Holztür in die Schmiede erscheint wie das Tor zu einer anderen Welt. Funken sprühen durch die Luft, als ob sich die Gischt in der Brandung am Fels entlädt. Der Geräuschpegel trägt kaum einen Wortfetzen bis ans Ohr. Der schwere Hammer donnert in rhythmischer Konstanz auf das glühende Eisen, plättet den Riegel glatt wie ein Küchenbrett. Wattestöpsel schützen die Gehörgänge, Lederhandschuhe Hände und Finger, die Sicherheitsschuhe Füße vor Funkenschlag und fallendem Eisen.

Schmiede seit 1686

Eine Waidlapfanne ist eine Bratpfanne, geschmiedet aus einem Stück. Ihre handwerkliche Herstellung verlangt viel Erfahrung, woran es an dieser Esse garantiert nicht mangelt. Seit über 300 Jahren schürt hier am Fuß der Bergstadt Schmiede-Generation um Schmiede-Generation das Feuer und bearbeitet mit Amboss, Hammer und Hitze das Metall. 1686 taucht die Schmiede erstmals in Urkunden auf. Für den Laien scheint sich auf den ersten Blick bis heute kaum etwas verändert zu haben. Die Hämmer werden heutzutage von Pressluftmotoren angetrieben und nicht mehr von Wasserkraft wie einst. Aber ansonsten? Ausstanzen, Anschweißen oder gar Zusammenschrauben – „das geht gar nicht!“, sagt Junior-Chef Stefan, der erste Schmied in der Ahnenfolge mit einem Bachelor in Maschinenbau. Jedes Stück aus dieser Werkstatt ist ein Unikat, aus einem Stück Eisen geformt und mit den Initialen der Familie geadelt.

Faszinierende Präzision

„Aller Anfang beginnt mit dem Stiel“, den Senior-Schmied Josef Kindermann aus dem schmalen Roheisen zieht. Der Weg zurück von der Technischen Hochschule in das traditionsreiche Familienhandwerk im Bayerischen Wald fiel seinem Sohn Stefan nicht schwer. „Hier bin ich mein eigener Chef“, weiß dieser. Der Erfolg gibt ihm recht. Die Bestelleingänge für die handgeschmiedeten Meisterstücke, mit denen sein Vater vor 25 Jahren begann, lassen den Computer für die

Bestelleingänge beinahe so heiß glühen, wie das Eisen in der Esse.

„10.000“ Pfannen“ habe er in seinem Leben bestimmt schon geschmiedet, sagt der junge Schmied. In drei verschiedenen Größen stellen er und sein Vater ihre exklusiven Bratpfannen her. „Das rechnet sich nach dem Durchmesser“, sagt Stefan Kindermann. Mit 17 und 28 Zentimeter Bratfläche hatte sein Vater die damals neuen Produkte ins Schmiedeportfolio aufgenommen, das vorher vor allem Werkzeuge, Messer und Gartengerät listete. Auch das stellen sie nach wie vor in Handarbeit her. Der Juniorschmied setzte eine Pfanne mit 32 Zentimeter Durchmesser obendrauf, die Jumbo-Pfanne. „Die ist zum echten Renner geworden“, freut er sich und lässt das Eisen nochmals glutrot leuchten, bevor er die runde Bodenplatte mit faszinierender Präzision aus dem breiten Teil des Eisenrohlings hämmert. Ihre finale Pfannenform mit dem hochgezogenen Rand erhält sie schließlich unter einer mächtigen Presse.

Zum Schluss sprühen erneut die Funken, wenn Kindermann die Flex zum Feinschliff an sein Werkstück ansetzt und schließlich mit der Stahlbürste die Politur vollendet. Polieren, Kontrolle und schon ist das Küchengerät fertig – „aber nur fast“, hämmert sich der Seniorchef in sein Handwerk zurück.

„Erst wenn sie sauber eingebraten ist“, wird sie zu dem, was sie ausmacht: Ein handgeschmiedetes Meisterwerk, in dem Fleisch, Fisch oder Gemüse „einfach anders schmecken“. Ehrlicher, krosser, authentischer. Die gleichmäßige Hitzeverteilung bringt die Kochkunst auf den Punkt.

Kochgerät für Generationen

„Bis sich die natürliche Patina gebildet hat, braucht sie noch etwas mehr Öl als herkömmliche Pfannen, dafür aber auch später deutlich weniger Hitze“, klärt der Seniorchef auf, während er gutes Olivenöl in sein Werk gießt, bis der Boden bedeckt ist. Er schneidet eine rohe Kartoffel in Scheiben, erhitzt langsam das Öl, verteilt die Kartoffel und einen EL Salz im Pfannenrohling und lässt schließlich alles bei mittlerer Hitze goldbraun braten. „So wird das gemacht“, sagt er, dreht das sauber geformte Stück Eisen nach dem Einbraten nochmals prüfend im Gegenlicht und stellt die Waidlapfanne schließlich ab in der Gewissheit: „Bei guter Pflege ist sie ein Kochgerät, von dem noch die Enkel etwas haben“.

Ein Schuh für harte Arbeit

Eine Waidlapfanne hält garantiert länger als die besten Sicherheitsschuhe, die sie in der Schmiede je getragen haben. Diesbezüglich müsste man den Kindermanns uneingeschränkt rechtgeben. Aber was würden sie sagen, wenn ihre Schuhe aus einem Stück Eisen geformt wären und das Gewicht einer Waidlapfanne hätten? Haix tragen die beiden mit Vorliebe und der neue Connexis Safety+ in Leder passt vom ersten Moment an wie angegossen.

Er ist der robuste Sicherheitsschuh mit einem echten Plus, den Haix genau für sol-

Bitte umblättern ▶

◀◀ zurück zum Inhaltsverzeichnis

che Einsätze und solche Berufsfelder entwickelt hat. Ein Sicherheitsschuh, der nicht nur Schutz auf dem Niveau von Sicherheitsklasse-S3 bietet, sondern zusätzlich mit der patentierten Connexis-Technologie von Haix ausgestattet ist.

Ein Plus für die Gesundheit

Neben den offensichtlichen Verletzungsgefahren sind Beschäftigte im Handwerk auch den nicht- oder weniger sichtbaren Gefahren ausgesetzt. Nur als Beispiel: Ungünstige Körperhaltung oder etwa andauerndes Stehen können sich dauerhaft negativ auf den Bewegungsapparat auswirken. Um dies zu reduzieren, stimuliert die im Connexis Safety+ integrierte Technologie aktiv die Faszien. Der Humanbiologe und Faszienforscher Dr. Robert Schleip erklärt dies folgender Maßen: „Faszien sind ein faseriges Netz aus Bindegewebe, das Muskeln, Organe sowie Knochen umhüllt und großen Anteil an unseren Bewegungen und unserer Beweglichkeit hat. Herkömmliche Schuhe versteifen den Fuß oft wie ein Gipsverband. Weil sie nicht ausreichend beansprucht werden, können die Faszien dadurch verfilzen. Das kann wiederum zu Schmerzen führen."

In die Schuhkonstruktion des Connexis Safety+ ist ein Tape integriert, das die Fußwurzel umfasst. Je nach individueller Einstellung übt es leichten Druck auf die Faszien in der Fußsohle aus. Ein Vorgang, den man von einer Faszienrolle kennt, auf der man mit der Fußsohle hin und her wippt. Das hat zur Folge, dass die Muskulatur positiv aktiviert wird. Gleichzeitig regt es den Blutfluss an. Die Folge: Negative Belastungen und deren Auswirkungen auf den Bewegungsapparat werden reduziert zugunsten von mehr Leistungsfähigkeit.

Ein Gewinn in Sachen Komfort

Damit der Fuß sich frei entfalten kann, ist der Connexis Safety+ an die natürliche Fußform angepasst. Das sorgt nicht nur für ein Plus an Komfort, sondern gibt den Füßen mehr natürliche Stabilität und beugt Fehlstellungen vor.

Trotz Faszien-Technologie und S3 Sicherheit ist der Schuh sehr leicht. Die Hightech Nano-Carbon-Zehenschutzkappe trägt dazu ihren Teil bei. Die rutschfeste und doch leichte Sohle mit ihrer speziell entwickelten Profilgestaltung gibt selbst auf rutschigen Untergründen guten Halt. In der Schmiede, wo Funken sprühen und es an anderen Stellen vom Kühlwasser feucht ist, besonders wichtig. Und noch eines ist nicht nur den Schmieden im Bayerischen Wald wichtig: Wie alle Produkte von Haix wird auch der Connexis Safety+ ausschließlich in Europa hergestellt. Dafür setzt das Unternehmen auf eigene, moderne Produktionsanlagen in Deutschland und Kroatien, wo höchste Standards bei Arbeitsbedingungen und Produktqualität selbstverständlich sind. Denn Made in Europe steht bei Haix nicht nur für das Plus an Qualität. Es ist auch ein Bekenntnis zu fairen Arbeitsbedingungen und zu mehr Nachhaltigkeit. ●

Vom Stahlrohling zur Pfanne: In rauen Umgebungen sind Sicherheitsschuhe der Sicherheitsklasse S3 wie der Haix Connexis Safety+ ein absolutes Muss

Die rutschfeste und doch leichte Sohle mit ihrer speziell entwickelten Profilgestaltung gibt selbst auf rutschigen Untergründen guten Halt

Autor
Hanno Meier
Selbstständig, Freier Redakteur,
PR, Communications und Consulting
m.press media

Haix Schuhe Produktions und Vertriebs-GmbH
Mainburg
Tel.: +49 8751 8625-0
info@haix.de
www.haix.com

A+A und Glasstec unter neuer Leitung

Lars Wismer (49) ist der führende Kopf der A+A sowie der Leitmesse der Glasbranche Glasstec geworden. Als Director verantwortet er neben den Leitmessen auch das internationale Portfolio Occupational Safety & Health mit den Messen TOS+H, CIOSH und OS+HA sowie das internationale Portfolio Glass Technologies mit den Messen Glasspex und Glasspro für den indischen Markt.

Lars Wismer

Er freue sich darauf, wieder an Bord der Messe Düsseldorf zu sein und gemeinsam mit einem starken Team die führende Position der beiden Leitmessen und die internationalen Portfolios weiter auszubauen, so Lars Wismer.

Lars Wismer ist bei der Messe Düsseldorf ein bekanntes Gesicht. Durch seine 16-jährige Tätigkeit als Senior Project Manager kennt er die Messe Düsseldorf sehr gut. Zusätzlich hat er eine umfangreiche Erfahrung im Management und in der Vermarktung von großen, internationalen Veranstaltungen. Zuletzt leitete er bei der D.Live GmbH & Co. KG als Executive Director Sports die Bereiche D.Sports Events, Sales, PR/Kommunikation und Marketing.

Petra Cullmann, Executive Director bei der Messe Düsseldorf, freue sich sehr, dass Lars Wismer für die Messe Düsseldorf zurückgewonnen werden konnte. Er habe langjähriges Know-how in der Leitung von internationalen Veranstaltungen im In- und Ausland. Die A+A und der 38. A+A Kongress für Arbeitsschutz und Arbeitsmedizin finden vom 24. bis 27. Oktober 2023 in Düsseldorf statt und stehen ganz im Zeichen der großen Megatrends Nachhaltigkeit und Digitalisierung.

www.messe-duesseldorf.de

◄◄ zurück zum Inhaltsverzeichnis

DBL: Andreas Iser wird Geschäftsführer

Der 48-jährige Andreas Iser startet als DBL Geschäftsführer für Finanzen und Organisation. Damit ist der Startschuss zum Umbau der DBL Geschäftsführung gegeben – und die Weichen in Richtung einer neuen Struktur im Verbund gestellt. Andreas Iser wechselt aus dem Vorstand des Metzgereifachgroßhandels Evenord in die Geschäftsführung der DBL – Deutsche Berufskleider-Leasing GmbH. Seine Karriere begonnen hat er beim Handelsriesen Metro, wo er mit 26 Jahren als einer der jüngsten Betriebsleiter des Konzerns reüssierte und rasch weiter aufstieg. Nach Management-Stationen als CFO beim Lebensmittelfachgroßhändler Omega Sorg und als Global Head of Business Development beim damaligen

© DBL – Deutsche Berufskleider-Leasing GmbH

Andreas Iser, neuer DBL Geschäftsführer für Finanzen und Organisation

Textil-Start-Up Naketano folgte der schnelle Aufstieg bei Evenord, wo er als Geschäftsführer und Vorstand verantwortlich für Finanzbuchhaltung, Controlling und Unternehmensstrategie zeichnete.

www.dbl.de

Warnschutzkleidung im Mietservice

Der textile Mietdienstleister DBL – Deutsche Berufskleider-Leasing GmbH hat normkonforme Warnschutzkollektionen im Programm. Die dunkle Jahreszeit ist da – für viele Profis Zeit, verstärkt Warnschutzkleidung zu tragen. Denn es geht darum, sichtbar zu bleiben. Bei jedem Wetter. Die Kleidung entspricht der aktuellen DIN EN ISO 20471 und gewährleistet die gewünschte 360°-Sichtbarkeit. Zudem sind zahlreiche neue Ergänzungsartikel erhältlich, die sich damit gut kombinieren lassen. Für die Betriebe sei es wichtig, ihre Mitarbeiter bei jedem Wetter flexibel auszurüsten – genau das werde mit den Ergänzungsartikeln möglich gemacht, so Thomas Krause von der DBL. Neu sind hier komfortable Wetterschutzjacken unter-

© DBL

Warnschutzkleidung von DBL

schiedlicher Länge, die zusammen mit den kombinierbaren Fleecejacken wetterfest und wintertauglich sind.

www.dbl.de

Material-Transportpaletten

Die Material-Transportpaletten Typ MTP von Bauer sind zum sicheren Lagern, Verladen und Transportieren von Gütern geeignet, wie z. B. von Transportgeräten. Sie zeichnet eine dreiseitige stabile Rahmenkonstruktion aus, die Wände bestehen aus Drahtgitter. Stirnseitig ist eine klappbare Auffahrrampe angebracht, die bei der Version MTP 3000 mit Gaszugfedern ausgestattet ist. Die Material-Transportpaletten

© Bauer GmbH

haben einen Tränenblechboden mit Einfahrtaschen zur Aufnahme mit einem Gabelstapler. Auch Sonderausführungen sind lieferbar.

www.bauer-suedlohn.de

◄◄ zurück zum Inhaltsverzeichnis

Drägerwerk: Umsatz und Ergebnis deutlich unter Vorjahr

Trotz weiterhin hohen Auftragsbestands blieb der Umsatz von Dräger im Geschäftsjahr 2022 hinter den Erlösen des Vorjahres zurück. Aus dem durchgängig hohen Auftragsbestand konnte aufgrund der erheblichen Störungen der globalen Lieferketten nicht im üblichen Umfang Umsatz generiert werden. Wegen der eingeschränkten Verfügbarkeit bestimmter elektronischer Bauteile, unter anderem aufgrund der coronabedingten Lockdowns an wichtigen Handelsplätzen in China, konnten einige Produkte nicht fertigproduziert und daher auch nicht an Endkunden ausgeliefert werden. Infolgedessen konnten auch die möglichen Umsätze aus dem Verkauf dieser Produkte nicht realisiert werden. Mit rund 3,04 Mrd. Euro (12 Monate 2021: 3,33 Mrd. Euro) lag der vorläufig berechnete Umsatz von Dräger im Geschäftsjahr 2022 daher währungsbereinigt 11,6 Prozent unter dem Wert des Vorjahrs.

Das niedrigere Umsatzvolumen führte auch zu einem deutlichen Ergebnisrückgang. Das vorläufig berechnete Ergebnis vor Zinsen und Steuern (EBIT) lag bei rund -87 Mio. Euro (12 Monate 2021: 271,7 Mio. Euro). Ein weiterer Grund für das geringere Ergebnis war die geringere Bruttomarge in Höhe von rund 41 Prozent (12 Monate 2021: 46,3 Prozent). Diese ging zum einen durch den veränderten Produktmix infolge der schwächeren Nachfrage nach coronabezogenen Produkten zurück. Zum anderen wurde sie durch die höheren Kosten für die Beschaffung schwer verfügbarer elektronischer Bauteile belastet.

Der Auftragseingang stieg aufgrund einer guten Nachfrage währungsbereinigt um 2,9 Prozent auf rund 3,29 Mrd. Euro (12 Monate 2021: 3,09 Mrd. Euro). Dabei legte das Segment Sicherheitstechnik währungsbereinigt um 8,4 Prozent auf rund 1,31 Mrd. Euro zu (12 Monate 2021: 1,17 Mrd. Euro). Die Medizintechnik verzeichnete einen leichten währungsbereinigten Rückgang von 0,5 Prozent auf rund 1,98 Mrd. Euro (12 Monate 2021: 1,92 Mrd. Euro). Dabei wurde die geringere Nachfrage nach Beatmungsgeräten durch ein deutliches Auftragsplus in den anderen Produktbereichen nahezu ausgeglichen.

Für das laufende Geschäftsjahr erwartet das Unternehmen eine schrittweise Verbesserung der Verfügbarkeit von Vorprodukten und somit eine Verbesserung der Lieferfähigkeit. Dies würde auf Basis des hohen Auftragsbestands eine deutliche Beschleunigung der Umsatzrealisierung und damit – trotz der erwarteten höheren Beschaffungs- und Personalkosten – eine Rückkehr zu Wachstum und Profitabilität ermöglichen. Dräger rechnet für 2023 daher mit einem Umsatzanstieg zwischen 5,5 und 9,5 Prozent (währungsbereinigt 7,0 und 11,0) sowie einer EBIT-Marge zwischen 0,0 und 3,0 Prozent. Der Ausblick steht unter dem Vorbehalt, dass sich die aktuellen wirtschaftlichen Rahmenbedingungen nicht wesentlich verschlechtern und die Wechselkurse nicht wesentlich verändern.

www.draeger.com

© Fristads/Henrik Sandsjo

Webshop für Arbeitskleidung & Outdoor-Kollektion ▲

Fristads baut sein E-Commerce-Geschäft auf dem europäischen Markt mit einem Webshop in Deutschland weiter aus. Der Shop bietet das gesamte Sortiment an Arbeitskleidung sowie die Outdoor-Kollektion und erhöht die Anzahl der Webshops auf insgesamt vier. Dies sei eine Ergänzung zum Business-to-Business-Geschäft, die den Endkunden eine größere Auswahl an Produkten bietet, so Anders Hülse, Geschäftsführer von Fristads. Das Unternehmen eröffnete seinen ersten Webshop im Jahr 2018 in Schweden, Finnland folgte im Frühjahr 2021 und Dänemark im Herbst 2021. Der deutsche Shop ist der jüngste Zugang zum Online-Geschäft des Herstellers. Die Webshops bieten außerdem nützliche Inhalte wie Größenanleitungen, einen Pflege- und Reparaturbereich, Informationen über Zertifizierungen und inspirierende Geschichten.

www.fristadskansas.de

Der deutsche Webshop ist erreichbar unter https://www.fristads.com/de-de

Bereichsüberwacher unterstützt UEG-Infrarotsensoren

Der Radius BZ1 Bereichsüberwacher von Industrial Scientific unterstützt in seinem abnehmbaren SafeCore-Modul auch UEG-Infrarot-(IR)Sensoren. Mit dem energiesparenden IR-Sensor verlängere sich die Akkulaufzeit, was wiederum das Anwendungsspektrum und die Flexibilität erweitert. Mit dieser Sensorkonfiguration kann der Radius BZ1 umfassend für die Erkennung gefährlicher Gase bei der Zaunlinien- und Perimeterüberwachung, Heißarbeiten und anderen Anwendungen für die Bereichsüberwachung eingesetzt werden. www.eu.indsci.com

© Industrial Scientific

Der Bereichsüberwacher Radius BZ von Industrial Scientific

Kübler für den Grünen Knopf lizenziert

Paul H. Kübler Bekleidungswerk GmbH & Co. KG ist für den Grünen Knopf lizenziert worden. Nachhaltiges Wirtschaften unter Berücksichtigung gesellschaftlicher, ökonomischer und ökologischer Belange hat für Kübler einen hohen Stellenwert. Der Grüne Knopf stellt verbindliche Anforderungen, um Mensch und Umwelt im Produktionsprozess von Textilien zu schützen. Insgesamt müssen 46 anspruchsvolle Sozial- und Umweltkriterien eingehalten werden – von A wie Abwassergrenzwerte bis Z wie Zwangsarbeitsverbot. Das Besondere am Grünen Knopf ist, dass neben dem Produkt immer auch das Unternehmen als Ganzes überprüft wird. Damit ist der Grüne Knopf das erste staatliche Siegel, das systematisch prüft, ob Unternehmen in ihrer textilen Lieferkette ihrer menschenrechtlichen und ökologischen Sorgfaltspflicht nachkommen. Der Staat legt die Kriterien und Bedingungen für den Grünen Knopf fest. Unabhängige Prüfstellen kontrollieren deren Einhaltung.

www.kuebler.eu

◄◄ zurück zum Inhaltsverzeichnis

© Denios

Feiern trotz Regen: Die Grundsteinlegung zum neuen Denios Gebäude in China

Denios legt Grundstein für neues Gebäude in China

Die Denios SE hat im chinesischen Changzhou den Grundstein für ein neues Produktions- und Verwaltungsgebäude gelegt. Das Unternehmen setzt damit ein großes Ausrufezeichen, um zukünftig auf dem chinesischen Markt eine wichtige Rolle spielen zu können. Für den Hersteller bedeutet dieser Neubau den Umzug in ein neues Zuhause: Bereits seit 2016 ist das Unternehmen hier mit der Produktion von Brandschutzsystemen und anderen Arbeitssicherheitsprodukten aktiv – nach dem anfänglichen Start in der Stadt Taicang wird heute in angemieteten Hallen in Changzhou gearbeitet. Genau dort hat es nun den Spatenstich für das neue Gebäude gegeben – läuft alles nach Plan, dann ist im Sommer 2024 alles fertig. In einem ersten Bauabschnitt wird eine Fertigungsfläche von etwa 4.300 Quadratmetern entstehen, die später noch erweitert werden soll. Das Verwaltungsgebäude wird nach der kompletten Fertigstellung eine Größe von mehr als 1.500 Quadratmetern haben.

www.denios.de

Hymer-Steigtechnik auf der Logimat

Der Allgäuer Hersteller Hymer präsentiert auf der kommenden Logimat intelligente Steigtechniklösungen für den sicheren Zugang zu höher gelegenen Arbeitsplätzen. Die internationale Fachmesse für Intralogistik-Lösungen und Prozessmanagement findet vom 25. bis 27. April 2023 in Stuttgart statt. Mit im Messegepäck sind Hymer-Steigleitern – optional mit persönlicher Absturzsicherung oder neu mit RAL-Beschichtung – sowie Stufenstehleitern mit R13-Beschichtung und schließlich eine höhenverstellbare Wartungsbühne. „Die Logimat ist für uns die wichtigste Fachmesse im Jahr und mit die beste Gelegenheit, uns als erfahrener Partner der Logistikbranche zu präsentieren“, erklärt Christian Frei, Vertriebsleiter Steigtechnik bei Hymer-Leichtmetallbau. Am Messestand A13 in Halle 3 werden die Stufenstehleitern mit R13-Beschichtung zu sehen sein. Die

© Hymer

Beschichtung wurde speziell für den Einsatz in feuchten oder öligen Bereichen entwickelt.

www.hymer-steigtechnik.de

Logimat:
Halle 3/ Stand 3A13

STEIGTECHNIK

Leiter will gelernt sein

Rundumservice von Hailo: Schulungen, Wartungen und Prüfungen

Hailo Professional bietet seinen Kunden nicht nur vielfältige Produktlösungen im Bereich Leitersysteme und Steigtechnik an – der Spezialist für Sicherheit beim Steigen stellt auch ein breites Portfolio an Serviceleistungen bereit, um den Schutz der Mitarbeiter am Arbeitsplatz zu gewährleisten. Dazu gehört die stetige Schulung der Personen, die für die Nutzung, Prüfung und Wartung der Produkte verantwortlich sind.

Damit Mitarbeiter sich zielgerichtet und effizient fortbilden können, bietet Hailo verschiedene Schulungen und Trainings an – ob im hauseigenen Trainings-Center in Haiger, beim Kunden vor Ort, direkt auf der Baustelle oder gänzlich remote. Zusätzlich zu den Schulungen und Trainings für den sicheren Umgang mit Leitersystemen und Steigtechnik unterstützt Hailo Unternehmen und Mitarbeiter auch bei der gesetzlich vorgeschriebenen Prüfung betrieblich genutzter Produkte – sowohl mit der Qualifikation von „zur Prüfung befähigten Personen“ als auch mit der praktischen Prüfapp Hailo Inspect.

Steigtechnik sicher nutzen: Lernen von Experten

Im hauseigenen Trainings-Center in Haiger bietet Hailo zahlreiche Weiterbildungen für Fachleute wie Monteure, Servicetechniker, Sicherheitsbeauftragte, Projektmanager oder Planer an: zum einen Seminare und Trainings zum Thema Sicherheit, zum anderen Schulungen zur Montage und Anwendung der verschiedenen Werkzeuge. Teilnehmer lernen mithilfe verschiedener praktischer Übungen, ihre Arbeit mit Steig- und Leitersystemen in der Praxis technisch einwandfrei umzusetzen. Zudem werden wichtige theoretische Grundlagen vermittelt, um die Sicherheit bei Aufbau und Anwendung der Systeme zu gewährleisten. Alle Schulungen werden von Profis durchgeführt, die sich bestens mit den verschiedenen Produkten, deren Einsatzgebieten, Anwendungen und Montagen auskennen. Natürlich können neben den Angeboten in Haiger auch maßgeschneiderte Schulungen an den jeweiligen Standorten der Unternehmen gebucht werden.

Christoph Moll, Abteilungsleiter Hailo Professional Dienstleistungen & Neue Märkte

Qualifikationen zur Prüfung und Wartung: auch als E-Learning möglich

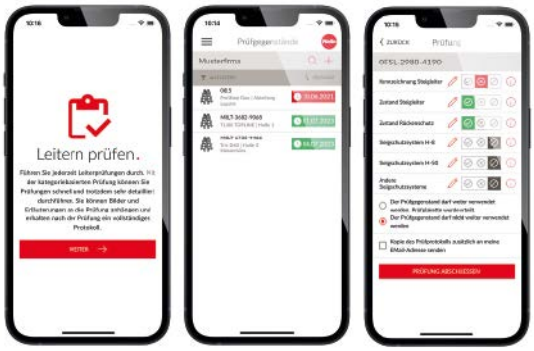
Wie alle Arbeitsmittel müssen auch betrieblich genutzte Leitern und Steigwege in regelmäßigen Intervallen auf ihren sicheren Zustand überprüft werden. Dazu zählen Leitern, Tritte, Fahrgerüste und ortsfest montierte Steigleitern einschließlich Steigschutzsystemen und Absturzsicherungen. Damit diese verantwortungsvolle Aufgabe von den Unternehmen selbst wahrgenommen werden kann, werden bei Hailo grundlegende gesetzliche und technische Kenntnisse zur Auswahl, Montage, Prüfung und Reparatur von Leitern auch per E-Learning-Programm vermittelt.

Auf der E-Learning-Plattform stellt Hailo Professional die Lehrgänge „Befähigte Person zur Prüfung von Leitern, Tritten und Fahrgerüsten“ sowie „Befähigte Person zur Prüfung von ortsfesten Steigleitern und Steigschutzsystemen“ zur Verfügung und bietet somit alle Vorteile, die zeitgemäßes E-Learning mit sich bringt: Die Kurse können jederzeit und ortsunabhängig durch-

◀ Wie alle Arbeitsmittel müssen auch betrieblich genutzte Leitern und Steigwege in regelmäßigen Intervallen auf ihren sicheren Zustand überprüft werden

geführt werden. Die Teilnehmer müssen nicht extra anreisen und können das Schulungsprogramm zeitlich individuell an ihren Arbeitsalltag anpassen. Das Programm ist Tag und Nacht verfügbar und kann jederzeit unterbrochen oder in kleineren Abschnitten abgearbeitet werden. Integrierte Zwischenprüfungen sorgen dabei für einen nachhaltigen Lernerfolg. Mit dem Bestehen eines Tests am Ende der Kurse qualifizieren sich die Teilnehmer für das Zertifikat. Damit versetzt das E-Learning-Programm seine Absolventen in die Lage, als „zur Prüfung befähigte Person nach Betriebssicherheitsverordnung" tätig zu werden.

Das E-Learning-Programm wird stetig ausgebaut und ist eine perfekte Ergänzung zu den Schulungen, die Hailo im Trainings-Center in Haiger oder In-House beim Kunden durchführt.



Digitale Leiterprüfung Hailo Inspect: Prüfgegenstände können per Foto dokumentiert und dem Prüfprotokoll hinzugefügt werden

Prüfungen und Wartungen als Service von Hailo Professional

Doch Hailo bildet Mitarbeitende von Unternehmen nicht nur als „zur Prüfung befähigte Person nach Betriebssicherheitsverordnung" aus – alternativ gibt es auch die Option, die eingesetzten Leitern direkt durch Hailo auf einen ordnungsgemäßen Zustand hin überprüfen zu lassen. Durchgeführt werden diese Wartungen und wiederkehrenden Prüfungen von fachkundigen Experten.

Hailo Inspect 2.0: App zur Prüfung von Leitern und Steigschutzsystemen

Zur erleichterten Dokumentation der Prüfung von Leitern kann zudem die digitale Leiterprüfung Hailo Inspect eine enorme Unterstützung sein. Seit 2019 hat die App laut Angaben des Herstellers zahlreiche Betreiber und Prüfer von betrieblich eingesetzten Leitern und Steigschutzsystemen überzeugt. Die Anwendung macht die regelmäßige Prüfung der Geräte deutlich komfortabler.

Erst kürzlich hat Hailo Inspect ein Update erhalten: Eine zusätzliche Desktop-Anwendung ermöglicht nun die geräteunabhängige Nutzung des Services. Darüber hinaus ist der Prüfvorgang in der Version 2.0 noch übersichtlicher gestaltet. „Wir haben es uns zur Aufgabe gemacht, Unternehmen im täglichen Arbeiten ganzheitlich zu unterstützen", sagt Christoph Moll, Abteilungsleiter Hailo Professional Dienstleistungen & Neue Märkte. „Der Service von Hailo Professional endet deshalb nicht beim Verkauf hochwertiger Produkte – sondern unterstützt deren Bereiber über die gesamte Verwendungsdauer hinweg. Mit der neuen Desktop-Anwendung ist die Nutzung von Hailo Inspect 2.0 geräteunabhängig und sogar offline möglich. Das sorgt für mehr Flexibilität. Außerdem haben wir die Prüfung auf einem Screen zusammengefasst – so sehen Prüfer alle nötigen Schritte auf einen Blick und können sie noch schneller abarbeiten."

Die Anwendung stellt alle Funktionen bereit, die der Betreiber sowie die „zur Prüfung befähigte Person nach Betriebssicherheitsverordnung" zur Überprüfung von Produkten wie mobilen Leitern und Tritten, ortsfesten Steigleitern sowie Steigschutzsystemen benötigen. Geräte können digital inventarisiert und verwaltet werden – auch solche von anderen Herstellern. Eine Erinnerungsfunktion macht auf anstehende Prüfungen aufmerksam. Mängel an den Prüfgegenständen können per Foto dokumentiert und dem Prüfprotokoll hinzugefügt werden. Das entsprechende Protokoll wird dem Betreiber – und optional auch dem Prüfer – nach Abschluss der Prüfung per E-Mail zugesandt. Der Zugriff auf bereits abgeschlossene Prüfungen ist darüber hinaus jederzeit möglich. Und dank der papierlosen Abwicklung leistet Hailo Inspect 2.0 auch einen Beitrag zur betrieblichen Nachhaltigkeit.

Ein anschauliches Onboarding macht neue Nutzer der App mit allen wichtigen Funktionen vertraut – so fällt der Einstieg besonders leicht.

Hailo Inspect 2.0 ist als App für die Betriebssysteme Android und iOS sowie als Desktop-Anwendung auf **Hailo-inspect.de** erhältlich. Die Anwendung steht in den Sprachen Deutsch und Englisch zur Verfügung und ist derzeit kostenlos. ●

Hailo-Werk
Haiger
Tel.: +49 2773 82 0
www.hailo.de

STEIGTECHNIK

Sicher in jeder Höhe

Passenden Höhenzugang ermitteln, Effizienz und Arbeitssicherheit fördern

Die Welt wird schnelllebiger, Prozesse werden komplexer und der Zeitdruck höher. In der Folge müssen Abläufe optimiert werden, um innerhalb kürzester Zeit ein Maximum an Produktivität zu ermöglichen. Damit steigen die Anforderungen an den Arbeitsschutz – Arbeitgeber müssen hier klare Auflagen erfüllen.

Dies gilt insbesondere für Wartungs- und Instandhaltungsaufgaben in der Höhe. Erhebungen der Deutschen Gesetzlichen Unfallversicherung zeigen: Jedes Jahr geschehen tausende Arbeitsunfälle. Abstürze gehören dabei zu den gefährlichsten Vorfällen. Die Gründe dafür sind meist Unachtsamkeit, falscher Einsatz oder grundsätzlich ungeeignete Zustiegslösungen für den geplanten Arbeitseinsatz.

Risikoanalyse: Zugangslösungen und Arbeitseinsatz unter gültigen Normen

Um Unfälle zu vermeiden, ist die Wahl des passenden Höhenzugangs deshalb entscheidend. Simone Harrer, Product Manager Ladders & Stepstools bei Zarges, beschäftigt sich intensiv mit den gültigen Normen und Sicherheitsvorgaben und weiß, wie Unfallrisiken bei Arbeiten in der Höhe erfolgreich verringert werden können. Sie sagt: „Mit einer Gefährdungsbeurteilung wird die am besten geeignete Zugangslösung für den geplanten Arbeitseinsatz ermittelt."

Wichtig für die sichere Arbeit in der Höhe ist eine für den Einsatz geeignete Leiter. Um den passenden Höhenzugang für den geplanten Einsatz ermitteln zu können, muss zuvor eine Gefährdungsbeurteilung durchgeführt werden. „Um zu wissen, wo beim Thema Arbeitssicherheit und Arbeitsschutz ange-

Schulungen für Anwender und Unternehmen

Als Spezialist von Zustiegslösungen beraten Experten von Zarges im Rahmen der Working at Height Consultation Anwender und Unternehmen zu geltenden Normen und Vorschriften, Unfallprävention und passender Ausstattung. Jetzt Beratung in Anspruch nehmen:

www.zarges.com/de/zarges-working-at-height-consultation

Stabilität und ein sicheres Standgefühl sind für die sichere Arbeit in der Höhe entscheidend

◄◄ zurück zum Inhaltsverzeichnis

Weitere Informationen zur TRBS-konformen Mehrzweckleiter Zarges Skymaster Plus X unter: https://www.zarges.com/de/trbs-2121-2/

setzt werden muss, ist eine Risikoanalyse der geplanten Tätigkeiten eine verpflichtende, aber auch strategisch wichtige Grundlage“, erläutert Harrer. Dabei werden die Rahmenbedingungen und gültigen Verordnungen ebenso analysiert wie die geplanten Arbeitsbereiche und Tätigkeiten. Auf dieser Basis werden sogenannte Schutzziele entwickelt und im nächsten Schritt die erforderlichen Maßnahmen geplant und umgesetzt. Darunter fällt auch die Wahl des passenden Steiggeräts, das zu der Aufgabe, den Umgebungsbedingungen und dem Arbeitsort passen muss.

TRBS 2121-2 und DIN-EN 131

Bei der Beschaffung gilt es zudem, eine Reihe an Vorgaben zu berücksichtigen. Hierzu zählen etwa die Technischen Regeln für Betriebssicherheit (TRBS 2121), Teil 2 „Gefährdung von Beschäftigten bei der Verwendung von Leitern“. Diese Richtlinie gibt etwa vor, dass Arbeiten auf Leitern nur auf Stufen oder Plattformen ausgeführt werden dürfen. Die Nutzung von Sprossen ist ausschließlich für den Verkehrsweg gedacht. Die TRBS-2121-2-Richtlinien ergänzen und konkretisieren die Vorgaben der Betriebssicherheitsverordnung (BetrSichV).

DIN-Normen wie die DIN-EN 131 geben die Rahmenbedingungen für sichere Höhenzugänge vor. So müssen etwa Leitern mit einer Länge von über drei Metern eine angemessen große Standbreite haben, damit der Anwender sicher steht. Hersteller wie Zarges nutzen für eine optimal große Standbreite Quertraversen.

TRBS-konforme Kombileiter

„Damit Unternehmen und Anwender sich keine Sorgen um die Sicherheit und Regularienkonformität machen müssen, haben wir mit der Skymaster Plus X eine dreiteilige Mehrzweckleiter entwickelt, die all diesen Anforderungen entspricht. Aufgrund der hybriden Bauweise sieht der Anwender sofort, ob er sich auf einer TRBS-konformen SaferStep-Stufe für den Arbeitsbereich oder einer Sprosse für den Verkehrsweg befindet. Für einen sicheren Stand wurden 80 Millimeter breite Stufen verbaut. Stabilität und ein sicheres Standgefühl sind für die sichere Arbeit in der Höhe ebenfalls entscheidend. Das haben wir mit beidseitig starren Verbindungen sowie einem insgesamt soliden Aufbau der Leiter aus hochwertigem Aluminium geschafft“, erläutert Simone Harrer den Entwicklungsprozess der TRBS-konformen Kombileiter bei Zarges.

Leiter-Handhabung muss einfach sein

Anwenderfreundlichkeit ist ein wichtiger, aber oftmals vernachlässigter Aspekt von Arbeitssicherheit. „Die sicherste, TRBS-konforme Leiter erfüllt ihren Zweck nicht, wenn die Handhabung zu umständlich ist. Besonders unter Zeitdruck greifen Anwender womöglich zu einer unsicheren Zwischenlösung oder Methode. Das erhöht das Risiko von Arbeitsunfällen und insbesondere Abstürzen, trotz zuvor getroffener Sicherheitsvorkehrungen“, erläutert Simone Harrer weiter. Neben einer soliden, vorgabenkonformen Fertigung sind deshalb auch eine einfache Handhabung und größtmögliche Ergonomie entscheidend bei der Wahl der richtigen Leiter.

„Bei der Entwicklung der Skymaster Plus X haben wir deshalb lange am Aufbau der Leiter gearbeitet. Sie sollte TRBS-konform sein und größtmögliche Sicherheit bieten, aber auch leicht im Gewicht und in der Handhabung“, so Harrer. Die Sicherheit sollte nicht zulasten des Anwenders gehen – deshalb wiegt die Hybridleiter trotz breiter Stufen und robustem Aufbau lediglich 18,8 Kilogramm bei einer Höhe von 5,80 Metern. Damit lässt sich die Leiter einfach umbauen und mit nur einer Hand transportieren. Die andere Hand bleibt frei, etwa für den Werkzeugkoffer. Denn auch durch das Vermeiden von Mehrfachgängen lassen sich Ermüdungserscheinungen und damit Sicherheitsrisiken vermeiden.

Investieren zur Unfallprävention

„Unternehmen sollten, auch aus wirtschaftlichen Gründen, bereits ein paar Jahre vorausdenken“, erklärt Harrer abschließend. Wenn also mit dem Jahreswechsel die Bestandsaufnahme und Neuanschaffung für die Ausstattung bei Wartungs- und Instandhaltungsaufgaben ansteht, lohnt es sich in eine Leiter für höchste Ansprüche bei der Arbeitssicherheit zu investieren – die Anforderungen an Arbeitgeber und Verantwortliche im Bereich Arbeitssicherheit werden zunehmend höher. So können Unternehmen sicher sein, sowohl hinsichtlich der optimalen Arbeitsunterstützung als auch bei der Unfallprävention auf der sicheren Seite zu sein. ●

Der Skymaster Plus X sorgt für gute Handhabung und ergonomischen Transport

© Bilder: Zarges

Zarges GmbH
Weilheim
Tel.: +49 881 687 0
zarges@zarges.de
www.zarges.de

◄◄ zurück zum Inhaltsverzeichnis

Virtueller Showroom eröffnet

Die Denios SE öffnet die Türen ihres virtuellen Showroom. Durch diesen können Kunden bequem hindurchspazieren. Auf diese Weise ist es möglich, die Produkte des Herstellers in qualitativ hoher 3D-Optik kennenzulernen und quasi virtuell „anzufassen“. Der virtuelle Showroom sei ein weiterer, wichtiger Baustein der Digitalisierungsstrategie des Unternehmens, so Marcus Schmitt, der bei Denios als Director Catalogue Products tätig ist. Die Kunden wünschten sich einen immer größeren, digitalen Service und Support – genau den liefere der Hersteller mit seiner neuen Anwendung. Öffnungszeiten gebe es dabei nicht, die Türen zum Showroom stehen immer offen.

Dabei ist ein Spaziergang durch die virtuellen Welten des Unternehmens leicht: Über die Homepage gelangt der Nutzer direkt in einen virtuellen Empfangsbereich, von dem aus die Wege in verschiedene Bereiche des Unternehmens führen. Per Mausklick oder Fingertipp wandert man nun durch den Showroom und kann sich dort nach Belieben

© Denios

Sieht aus wie echt: Der digitale Showroom von Denios

auf einzelne Produkte zubewegen: Auffangwannen, Gefahrstoffschränke, Brandschutzsysteme und mehr – der Showroom bietet viel Platz für die verschiedensten Lösungen des Herstellers.

Das Besondere: Die Produkte selbst sind alle in 3D-Optik aufbereitet worden und können vom Kunden quasi „in die Hand genommen werden“. Egal ob detailreiches Heranzoomen an ein Objekt oder ein 360-Grad-Rundumblick – im Showroom bekommt man das Gefühl, direkt vor den Produkten zu stehen und sie hautnah zu erleben. Darüber hinaus können weitere Informationen abgerufen werden: Datenblätter, Videos zu den Produkten – die virtuelle Welt macht es möglich, dass sich der Kunde in allen Belangen über das umfangreiche Portfolio des Herstellers informieren kann.

Neben der klassischen Produktwelt können die Kunden außerdem in die digitalen Serviceleistungen des Unternehmens eintauchen, so Marcus Schmitt. Wer mehr zum Thema Gefahrstofflagerung wissen möchte, sei im Showroom genauso gut aufgehoben wie jemand, der sich über Denios connect informieren möchte. Dabei handelt es sich um eine Gefahren-Echtzeit-Überwachung, die in Raumsystemen und Gefahrstoffschränken zum Einsatz kommt.

Genau diese zwei Varianten machten die virtuelle Denios-Welt so attraktiv und spannend, so Marcus Schmitt. Entweder erkundet man auf eigene Faust das große Portfolio oder man vereinbart im Vorfeld einen Beratungstermin und wird sich dann mit einem Showroom-Experten gemeinsam durch die einzelnen Räume bewegen. Das Ganze funktioniert per Videochat und bietet einen weiteren Vorteil: Bei Fragen steht der Experte sofort zur Seite und kann somit beraten und weiterhelfen. Sind alle wichtigen Dinge geklärt, kann der Kunde per Mausklick direkt in den Web-shop gehen und dort das gewünschte Produkt kaufen. Ein digitaler Rund-um-Service für die Kunden, die sich auf virtuelle Art und Weise vom ersten Eindruck der Produkte über die Beratung bis hin zum Kauf komplett in der digitalen Welt bewegen können.

www.denios.de

Arbeitshose mit anpassbarer Pro Werkzeugtasche

Die Workwear-Marke Schöffel Pro baut ihr Angebot an hochfunktionellen, robusten Arbeitshosen aus. Die vier Arbeitshosen-Modelle der neuen Generation sind nun zusätzlich zu den Farben Blau, Grau und Grün auch in der Trendfarbe Schwarz erhältlich. Herzstück der Arbeitshosen-Kollektion ist die Pro Werkzeugtasche, die sich an die individuellen Anforderungen des Trägers anpassen lässt. Ob für die permanente Aufbewahrung von Werkzeug, das schnell verfügbar sein muss, oder nur für den gelegentlichen Einsatz des Zollstocks – die Pro Werkzeugtasche bietet für jeden die passende Lösung. Die einzippbare und bei Bedarf herausklappbare Pro Werkzeugtasche bietet fünf Einsteckfächer und ein Zollstockfach. Eine große, umlaufende Reißverschlusstasche schützt das Werkzeug vor Verlust. Wenn kein Werkzeug benötigt wird, kann die Pro Werkzeugtasche einfach und schnell abgezippt und dank ihres sportlichen Looks auch nach Feierabend getragen werden.


© Schöffel

www.invista.com

Recycelte Laminate für Arbeitsschutzbekleidung

Nachhaltige Materialien und Produktionsprozesse von Gore-Tex Professional (Gore) sparen CO_2 und Wasser. Der ökologische Fußabdruck der wasserdichten, winddichten und atmungsaktiven Soft Gore-Tex Shell Technologie wird durch drei Hebel stark reduziert – durch die Langlebigkeit der Materialien, Verwendung von Textilien aus recycelten PET-Flaschen und Nutzung eines textilen Rundstrick- und Spinndüsenfärbeverfahrens. Insgesamt führt das zu einer CO_2-Einsparung von fast 54 %, einem um etwa 64 % geringeren Wasserverbrauch und einem reduzierten Einsatz von Chemikalien. Das eingesetzte Rundstrickverfahren minimiert nicht nur die CO_2-Emissionen deutlich, sondern ermöglicht auch ein angenehm weiches Hardshell Laminat. Das Innenfutter des Laminats ist im Spinndüsenverfahren gefärbt. Bei diesem Verfahren


© Gore/Joachim Stark

Soft Gore Tex Shell

wird der Farbstoff dem Polymer zugesetzt, bevor das Garn gesponnen wird. Da keine weiteren Färbeprozesse erforderlich sind, wird der Verbrauch von CO_2, Wasser und Chemikalien erheblich reduziert.

www.gore.com

◄◄ zurück zum Inhaltsverzeichnis


© Pepperl+Fuchs

Vorstand Pepperl+Fuchs SE

Pepperl+Fuchs erreicht erstmals die Milliarden-Marke

Zum ersten Mal in seiner 77-jährigen Firmengeschichte hat es Pepperl+Fuchs geschafft, die Schwelle von weltweit einer Milliarde Euro Jahresumsatz zu überschreiten. Damit hat das Unternehmen sein ursprünglich für 2025 avisiertes Ziel deutlich früher als geplant erreicht – aller Widrigkeiten der letzten Krisenjahre zum Trotz. Tatsächlich konnte das global aufgestellte Unternehmen die Herausforderungen seit Beginn der Corona-Pandemie gut meistern. Nachdem der Umsatz im Jahr 2020 zunächst um 9 % zurückging, konnte in den nächsten beiden Pandemiejahren eine Umsatzsteigerung von insgesamt mehr als 40 % verbucht werden. Dass dies ungeachtet der durch Pandemie, Lieferengpässe, teils drastischen Preisentwicklungen und nicht zuletzt den Krieg in der Ukraine sowie die Gasmangellage bedingten, enorm schwierigen Rahmenbedingung gelungen ist, macht Dr. Gunther Kegel, CEO der Pepperl+Fuchs Gruppe, sehr stolz.

www.pepperl-fuchs.com

Asecos: Tochtergesellschaft in Schweden

Die Asecos GmbH baut ihre Präsenz in Nordeuropa weiter aus. Dazu hat das Unternehmen auf dem skandinavischen Markt eine Tochtergesellschaft gegründet: die Asecos AB. Das Unternehmen ist am Standort Uppsala in Schweden vertreten. Durch die Gründung der schwedischen Tochtergesellschaft kann das Unternehmen seinen Kunden in Skandinavien mehr Möglichkeiten und Lösungen bieten. Nordeuropa und besonders Schweden hätten in den vergangenen Jahren enorm an Bedeutung für den Hersteller gewonnen. Die neue Gesellschaft in Uppsala stärke nicht nur die vertrieblichen Aktivitäten dort, sondern ermögliche auch einen besseren Zugang zu den anderen skandinavischen Ländern, so Günther Rossdeutscher, Geschäftsführer Asecos GmbH. Zu den bereits heute sechs Gesellschaften in den Niederlanden, Frankreich, Spanien, Großbritannien, USA und der Schweiz erweitert die Asecos AB als siebtes Tochterunternehmen die globale Marktpräsenz des hessischen Gefahrstoff-Experten.


© Asecos

Asecos Deutschland

www.asecos.com

◄◄ zurück zum Inhaltsverzeichnis

Liebe Leserinnen und Leser,

In BusinessPartner, dem „Who is who in Sachen Sicherheit", präsentieren sich Ihnen die kompetentesten Anbieter aus allen Sicherheitsbereichen. Die hier vertretenen Firmen legen Wert auf den Kontakt mit Ihnen. Alle Einträge finden Sie auch in www.git-sicherheit.de/buyers-guide mit Links zu den Unternehmen!

Sie gehören selbst zu den wichtigen Anbietern und wollen mit jeder Ausgabe 30.000 Entscheider direkt erreichen? Dann kontaktieren Sie uns für eine Aufnahme.

SICHERHEITS MANAGEMENT

Sicherheitsmanagement

BOSCH

Bosch Building Technologies
Robert-Bosch-Ring 5 · 85630 Grasbrunn
Tel.: 0800/7000444 · Fax: 0800/7000888
Info.service@de.bosch.com
www.bosch-Sicherheitssysteme.de
Produkte und Systemlösungen für Videoüberwachungs-, Einbruchmelde-, Brandmelde-, Sprachalarm- und Managementsysteme sowie Zutrittskontrolle, professionelle Audio- und Konferenzsysteme. In ausgewählten Ländern bietet Bosch Lösungen und Dienstleistungen für Gebäudesicherheit, Energieeffizienz und Gebäudeautomation an.

Sicherheitsmanagement

funkwerk

Funkwerk video systeme GmbH
Thomas-Mann-Str. 50 · D-90471 Nürnberg
Tel.: +49(0)911/75884-518
info@funkwerk-vs.com
www.funkwerk.com/videosysteme
CCTV, Systemlösung, Systemintegration, Videoüberwachung, Security, Gebäudemanagement

Sicherheitsmanagement

NSC Sicherheitstechnik GmbH

NSC Sicherheitstechnik GmbH
Lange Wand 3 · 33719 Bielefeld
Tel.: +49 (0) 521/13629-0
Fax: +49 (0) 521/13629-29
info@nsc-sicherheit.de · www.nsc-sicherheit.de
Brandmeldetechnik, Videotechnik, Sprach-Alarm-Anlagen

Sicherheitsmanagement

ABUS
Security Tech Germany

ABUS Security-Center GmbH & Co. KG
Linker Kreuthweg 5 · D-86444 Affing
Tel.: +49(0)8207/95990-0
Fax: +49(0)8207/95990-100
info.de@abus-sc.com · www.abus.com
ABUS Security-Center ist Hersteller innovativer Alarmanlagen, Videoüberwachungssysteme und Zutrittskontrollsysteme. Als Teil der ABUS Gruppe ist das Unternehmen sowohl auf branchenspezifische Sicherheitsbedürfnisse, als auch auf die Anforderungen von Privatanwendern spezialisiert.

Sicherheitsmanagement

DAITEM

Daitem / Atral Security Deutschland GmbH
Eisleber Str. 4 · D-69469 Weinheim
Tel.: +49(0)6201/6005-0
info@daitem.de · www.daitem.de
www.brandwarnanlage.de
Funk-Einbruch- und Brandschutzlösungen vom Technologieführer. Vertrieb über qualifizierte Sicherheitsfacherrichter.

Sicherheitsmanagement

Security Robotics®

Security Robotics Development & Solutions GmbH
Landsberger Allee 366 · 12681 Berlin
info@security-robotics.de · www.security-robotics.de
Robotics, Sicherheitstechnik, Autonomie, Qualitätssteigerung, Künstliche Intelligenz, Vernetzte Zusammenarbeit, SMA Unterstützung

Sicherheitsmanagement

Armantis®

Armantis GmbH
Seebachring 74 · 67125 Dannstadt
Tel.: +49 621 95 04 08 0
info@armantis.de · www.armantis.de
Systemanbieter Sicherheitstechnik. Produkte und Systemlösungen für Anforderungen im mittleren bis hohen Risikobereich: SMAVID Videoüberwachungstechnik, UNii Alarmsysteme, UR Fog Sicherheitsnebel, myTEM Gebäudeautomation.

Sicherheitsmanagement

deister electronic

deister electronic GmbH
Hermann-Bahlsen-Str. 11
D-30890 Barsinghausen
Tel.: +49(0)5105/516-111 · Fax: +49(0)5105/516-217
info.de@deister.com · www.deister.com
Zutritts- und Zufahrtskontrollsysteme; biometrische Verifikation; Wächterkontrollsysteme; Verwahrung und Management von Schlüsseln und Wertgegenständen

Sicherheitsmanagement

VSW
Vereinigung für die Sicherheit der Wirtschaft e.V.

Vereinigung für die Sicherheit der Wirtschaft e.V.
Lise-Meitner-Straße 1 · 55129 Mainz
Tel.: +49 (0) 6131 - 57 607 0
info@vsw.de · www.vsw.de
Als Schnittstelle zwischen den Sicherheitsbehörden und der Wirtschaft in allen Fragen der Unternehmenssicherheit steht die gemeinnützige Vereinigung seit 1968 der Wirtschaft als unabhängige Organisation zur Verfügung.

Sicherheitsmanagement

ASSA ABLOY
Opening Solutions

ASSA ABLOY Sicherheitstechnik GmbH
Bildstockstraße. 20 · 72458 Albstadt
www.assaabloyopeningsolutions.de
albstadt@assaabloy.com
Das Unternehmen entwickelt, produziert und vertreibt unter den traditionsreichen und zukunftsweisenden Marken IKON, effeff, KESO und Yale hochwertige Produkte und vielseitige Systeme für den privaten, gewerblichen und öffentlichen Bereich.

Sicherheitsmanagement

EVVA

EVVA Sicherheitstechnik GmbH
Höffgeshofweg 30 | 47807 Krefeld | Deutschland
T +49 2151 37 36-0 | F +49 2151 37 36-5635
office-krefeld@evva.com | www.evva.com

Föpplstraße 15 | 04347 Leipzig | Deutschland
T +49 341 234 090-5 | F +49 341 234 090-5760
office-leipzig@evva.com | www.evva.com

EVVA ist Entwickler und Hersteller von mechanischen aund elektronischen Zutrittssystemen.

GEBÄUDE SICHERHEIT

Sicherheitsmanagement

barox
Switche für Video

barox Kommunikation GmbH · 79540 Lörrach
Tel.: +49 7621 1593 100
www.barox.de · mail@barox.de
Cybersecurity, Videoswitch, PoE Power-over-Ethernet, Medienkonverter, Extender

Sicherheitsmanagement

FREIHOFF 24 GRUPPE

Freihoff Sicherheitsservice GmbH
Herzogstraße 8 · 40764 Langenfeld
Tel.: 02173 106 38-0
info@freihoff.de · www.freihoff-gruppe.de
Einbruchmeldeanlagen, Brandmeldeanlagen, Videoüberwachung, Zutrittskontrolle, Notruf- und Serviceleitstelle

Gebäudesicherheit

WINKHAUS

Aug. Winkhaus GmbH & Co. KG
Hessenweg 9 · 48157 Münster
Tel.: +49 251 4908-0 · Fax: +49 251 4908-145
zutrittsorganisation@winkhaus.de
www.winkhaus.de
Zutrittsorganisation, elektronische und mechanische Schließsysteme, Tür- und Fenstertechnik, Notausgangs- und Anti-Panik-Verriegelungen

Gebäudesicherheit

deister electronic GmbH
Hermann-Bahlsen-Str. 11
D-30890 Barsinghausen
Tel.: +49(0)5105/516-111 · Fax: +49(0)5105/516-217
info.de@deister.com · www.deister.com
Zutritts- und Zufahrtskontrollsysteme; biometrische Verifikation; Wächterkontrollsysteme; Verwahrung und Management von Schlüsseln und Wertgegenständen

Gebäudesicherheit

Uhlmann & Zacher GmbH
Gutenbergstraße 2-4 · 97297 Waldbüttelbrunn
Tel.: +49(0)931/40672-0 · Fax: +49(0)931/40672-99
contact@UundZ.de · www.UundZ.de
Elektronische Schließsysteme, modular aufgebaut und individuell erweiterbar

Gebäudesicherheit

Dictator Technik GmbH
Gutenbergstr. 9 · 86356 Neusäß
Tel.: 0821/24673-0 · Fax: 0821/24673-90
info@dictator.de · www.dictator.de
Antriebstechnik, Sicherheitstechnik, Tür- und Tortechnik

Gebäudesicherheit

Walter Wurster GmbH
Heckenrosenstraße 38-40
70771 Leinfelden-Echterdingen
Tel.: 0711/949 62-0 · kontakt@wurster-online.de
www.wurster-online.de · www.ideeninblech.de
Geldübergabeschalter feuerbeständig bis F90 und beschussshemmend bis FB7, Durchreichen für Geld, Wertsachen und Dokumente, Hochsicherheits-Durchreichen, Bankschalter, Nachtschalter, Tankstellenschalter, Apothekenschalter, Ticketschalter für Sport- und Kulturstätten

Videoüberwachung

ABUS Security-Center GmbH & Co. KG
Linker Kreuthweg 5 · D-86444 Affing
Tel.: +49(0)8207/95990-0
Fax: +49(0)8207/95990-100
info.de@abus-sc.com · www.abus.com
ABUS Security-Center ist Hersteller innovativer Alarmanlagen, Videoüberwachungssysteme und Zutrittskontrollsysteme. Als Teil der ABUS Gruppe ist das Unternehmen sowohl auf branchenspezifische Sicherheitsbedürfnisse, als auch auf die Anforderungen von Privatanwendern spezialisiert.

Gebäudesicherheit

DOM Sicherheitstechnik GmbH & Co. KG
Wesselinger Straße 10-16 · D-50321 Brühl / Köln
Tel.: + 49 2232 704-0 · Fax: + 49 2232 704-375
dom@dom-group.eu · www.dom-security.com
Mechanische und digitale Schließsysteme

Videoüberwachung

BURG-GUARD GmbH
Wormgermühle 1 · 58540 Meinerzhagen
Tel.: +49 2358/905 490 · Fax: +49 2358/905 499
Burg-Guard@burg.biz · www.burg-guard.com
Videosicherheit · Analog- & IP-Kameras
AI Videoanalyse · Netzwerkrekorder
BURGcam APP · Projektierung · Service & Support

Gebäudesicherheit

GEZE GmbH
Reinhold-Vöster-Str. 21-29 · D-71229 Leonberg
Tel.: 07152/203-0 · Fax: 07152/203-310
info.de@geze.com · www.geze.com
Flucht- und Rettungswegsysteme, Zutrittskontrollsysteme, RWA, Feststellanlagen

Perimeterschutz

Berlemann Torbau GmbH
Ulmenstraße 3 · 48485 Neuenkirchen
Tel.: +49 5973 9481-0 · Fax: +49 5973 9481-50
info@berlemann.de · www.berlemann.de
INOVA ist die Marke für alle Komponenten der Freigeländesicherung aus einer Hand! Als Qualitätshersteller für Schiebetore, Drehflügeltore, Zaun-, Zugangs- und Detektionssysteme haben Sie mit INOVA auf alle Fragen des Perimeterschutzes die passende Antwort.

Videoüberwachung

Ihr Value Added Distributor für Videosicherheitstechnik „Made in Germany“

Dallmeier Components GmbH
Hoheluftchaussee 108 | 20253 Hamburg
Tel. +49 40 47 11 213-0 | Fax +49 40 47 11 213-33
info@d-components.com | www.d-components.com

Gebäudesicherheit

SimonsVoss Technologies GmbH
Feringastr. 4 · 85774 Unterföhring
Tel.: 089 992280
marketing-simonsvoss@allegion.com
www.simons-voss.com
Digitale Schließanlagen mit Zutrittskontrolle, kabellose und bohrungsfreie Montage, batteriebetrieben, keine Probleme bei Schlüsselverlust.
Digital Schließen ist neu für Sie? Rufen Sie an: 089 99228-555

Perimeterschutz

CONDOR IMS GmbH
Ruhrtalstraße 81 · 45239 Essen
Tel.: +49 201 841 53-0
www.condor-ims.com
sekretariat@condor-sicherheit.de
Perimeter-Schutz | Sicherheitsdrohne | Automation | Alarm-Verifikation | Einbruchschutz

Videoüberwachung

Dallmeier electronic GmbH & Co. KG
Bahnhofstraße 16 · 93047 Regensburg
Tel.: 0941/8700-0 · Fax: 0941/8700-180
info@dallmeier.com · www.dallmeier.com
Videosicherheitstechnik made in Germany: Multifocal-Sensortechnologie Panomera®, IP-Kameras, Aufzeichnungsserver, intelligente Videoanalyse, Videomanagementsoftware

Gebäudesicherheit

Süd-Metall Beschläge GmbH
Sägewerkstraße 5 · D - 83404 Ainring/Hammerau
Tel.: +49 (0) 8654 4675-50 · Fax: +49 (0) 8654 4675-70
info@suedmetall.com · www.suedmetall.com
Funk-Sicherheitsschlösser made in Germany, Mechanische & elektronische Schließsysteme mit Panikfunktion und Feuerschutzprüfung, Zutrittskontrollsysteme modular und individuell erweiterbar, Systemlösungen, Fluchttürsteuerung

Perimeterschutz

Raytec Ltd.
Unit 15 Wansbeck Business Park · Rotary Parkway
Ashington, Northumberland · NE63 8QW, UK
Tel: +44 (0) 1670 520055
sales@raytecled.com · www.raytecled.com
Raytec LED-Beleuchtung für Ihre Sicherheit. Beleuchtungslösungen für die Bereiche Gefahrenzonen, Industrie, Transport und Sicherheit.

Videoüberwachung

EIZO Europe GmbH
Belgrader Straße 2
41069 Mönchengladbach
Tel.: +49 2161 8210 0
info@eizo.de · www.eizo.de
Professionelle Monitore für den 24/7-Einsatz in der Videoüberwachung, IP-Decoder-Monitore für den computerlosen Anschluss an IP-Kameras.

Videoüberwachung

AUS GUTEM GRUND GRUNDIG

Abetechs GmbH (Grundig Security)
Steinhof 39 · D-40699 Erkrath
Tel.: +49 211 5380 6832
info@grundig-security.com · www.grundig-security.com
Das neue Programm von GRUNDIG Security enthält alles, was Sie für eine moderne und professionelle Videoüberwachungsanlage benötigen.

Videoüberwachung

TKH GROUP TKH SECURITY

TKH Security GmbH
Max-Planck-Straße 15 a-c | D-40699 Erkrath
Tel.: +49 211 247016-0 | Fax: +49 211 247016-11
info.de@tkhsecurity.com | www.tkhsecurity.de
Videoüberwachung, Zutrittskontrolle, Sicherheitsmanagement, mobile Videoüberwachung und Videomanagement

Zeit + Zutritt

CDVI Security to Access

CDVI GmbH
Dahlweg 105 / Tor 2 · D-48153 Münster
Tel.: +49 (0)251 798 477-0
info@cdvi.de · www.cdvi.de
Zutrittskontrolle, Zutrittskontrollsysteme, Zutritt mittels Smartphone, Biometrische Systeme, Türautomation, Komponenten für Türen+Tore

Videoüberwachung

Hanwha Techwin Europe

Hanwha Techwin Europe Limited
Kölner Strasse 10
65760 Eschborn
Tel.: +49 (0)6196 7700 490
hte.dach@hanwha.com · www.hanwha-security.eu/de
Hersteller von Videoüberwachungsprodukten wie Kameras, Videorekorder und weiteren IP-Netzwerkgeräten. Sowie Anbieter von Software-Lösungen wie beispielsweise Videoanalyse, Lösungen für den Vertical-Market und Videomanagementsoftware (VMS).

Videoüberwachung

unv

Zhejiang Uniview Technologies Co., Ltd.
Building No.10, Wanlun Science Park,
Jiangling Road 88, Binjiang District,
Hangzhou, Zhejiang, China (310051)
info.dach@uniview.com · https://global.uniview.com
Uniview ist der führende Hersteller für Videoüberwachung mit kompletten Produktlinien für eine sicherere Welt. Wir stellen professionelle Kameras, Rekorder, Display Produkte etc. mit strengem Qualitätskontrollsystem für höhere Zuverlässigkeit her.

Zeit + Zutritt

cryptin CICHON STOLBERG

Cichon+Stolberg GmbH
Wankelstraße 47-49 · 50996 Köln
Tel.: 02236/397-200 · Fax: 02236/61144
info@cryptin.de · www.cryptin.de
Betriebsdatenerfassung, Zeiterfassung, cryptologisch verschlüsselte Zutrittskontrolle

Videoüberwachung

HIKVISION

HIKVISION Deutschland GmbH
Flughafenstr. 21 · D-63263 Neu-Isenburg
Tel.: +49 (0) 69/40150 7290
sales.dach@hikvision.com · www.hikvision.com/de
Datenschutzkonforme Videoüberwachung, Panorama-Kameras, Wärmebild-Kameras, PKW-Kennzeichenerkennung

ZEIT ZUTRITT

Zeit + Zutritt

deister electronic

deister electronic GmbH
Hermann-Bahlsen-Str. 11
D-30890 Barsinghausen
Tel.: +49(0)5105/516-111 · Fax: +49(0)5105/516-217
info.de@deister.com · www.deister.com
Zutritts- und Zufahrtskontrollsysteme; biometrische Verifikation; Wächterkontrollsysteme; Verwahrung und Management von Schlüsseln und Wertgegenständen

Videoüberwachung

i-PRO

i-PRO EMEA B.V.
Laarderhoogtweg 25 · 1101 EB Amsterdam
Netherlands
https://i-pro.com/eu/en
Hochwertige CCTV-Lösungen (IP & analog), Video-Automatisierung und KI, Technologien für hohe Ansprüche (FacePro, Personen-Maskierung), Schutz vor Cyber-Attacken im Einklang mit DSGVO, VMS: Video Insight

Zeit + Zutritt

AceProx Identifikationssysteme GmbH

AceProx Identifikationssysteme GmbH
Bahnhofstr. 73 · 31691 Helpsen
Tel.: +49(0)5724-98360
info@aceprox.de · www.aceprox.de
RFID-Leser für Zeiterfassung, Zutrittskontrolle und Identifikation

Zeit + Zutritt

ELATEC RFID Systems

ELATEC GmbH
Zeppelinstr. 1 · 82178 Puchheim
Tel.: +49 89 552 9961 0
info-rfid@elatec.com · www.elatec.com
Entwickler und Hersteller für zukunftssichere RFID Reader. Flexible Module für spezifische Lösungen (LF, HF, NFC, BLE). Unterstützt mehr als 60 Technologien und ist in über 100+ Ländern zertifiziert.

Videoüberwachung

www.luna-hd.de
lunaHD High Definition Video
Videoüberwachung • Türsprechanlagen

Zeit + Zutritt

AZS SYSTEM AG

AZS System AG
Mühlendamm 84 a · 22087 Hamburg
Tel.: 040/226611 · Fax: 040/2276753
www.azs.de · anfrage@azs.de
Hard- und Softwarelösungen zu Biometrie, Schließ-, Video-, Zeiterfassungs- und Zutrittskontrollsysteme, Fluchtwegsicherung, Vereinzelungs- und Schrankenanlagen, OPC-Server

Zeit + Zutritt

FEIG

FEIG ELECTRONIC GMBH
Industriestr. 1a · 35781 Weilburg
Tel.: +49(0)6471/3109-375 · Fax: +49(0)6471/3109-99
sales@feig.de · www.feig.de
RFID-Leser (LF, HF, UHF) für Zutritts- und Zufahrtskontrolle, Geländeabsicherung, Bezahlsysteme u.v.m.

Videoüberwachung

SECURITON IPS

Securiton Deutschland
IPS Intelligent Video Software
Kronstadter Str. 4 · 81677 München
Tel.: +49 89 4626168-0
ips@securiton.de · www.ips.securiton.de
Hersteller von high-end Videomanagementsoftware und intelligenter Videoanalysesoftware zur Echtzeiterkennung von potentiellen Gefahrensituationen.

Zeit + Zutritt

DoorBird Technology meets Design.

Bird Home Automation GmbH
Uhlandstr. 165 • 10719 Berlin
Tel. +49 30 12084892 • Fax: +49 30 120858695
hello@doorbird.com • www.doorbird.com
Zutrittskontrolle; Tür- und Tortechnik; Türkommunikation; Gebäudetechnik; IP Video Türsprechanlage; RFID; Biometrie; Fingerabdruck; Made in Germany

Zeit + Zutritt

Gantner

GANTNER Electronic GmbH
Bundesstraße 12 · 6714 Nüziders · Österreich
Tel.: +43 5552 33944
info@gantner.com · www.gantner.com
Systemlösungen in Zutrittskontrolle/Biometrie, Zeiterfassung, Betriebsdatenerfassung, Schließsysteme, Zugriffsschutz, Schrankschließsysteme

Zeit + Zutritt

IDEMIA Germany GmbH
Konrad-Zuse-Ring 1 · 24220 Flintbek
Tel.: +49 (0) 234 9787 0 · Fax: +49 (0) 4347 715 - 3101
biometric.devices@idemia.com · www.idemia.com
Zutrittskontrolle, Biometrie, Gesichtserkennung, Fingerabdruck, Video Analyse

Zeit + Zutritt

phg
Peter Hengstler GmbH + Co. KG
D-78652 Deißlingen · Tel.: +49(0)7420/89-0
datentechnik@phg.de · www.phg.de
RFID und Mobile Access: Leser für Zutrittskontrolle, Zeiterfassung, BDE, Türkommunikation, Besuchermanagement, Parksysteme, Zufahrtskontrolle, Vending, ... Terminals, Einbaumodule, Kartenspender, Tischlesegeräte, Leser für Markenschalterpogramme, Modbus-Module, Identifikationsmedien, ... einfach und komfortabel zu integrieren.

NOTRUF SERVICE LEITSTELLE

Zeit + Zutritt

iLOQ Deutschland GmbH
Am Seestern 4 · 40547 Düsseldorf
Tel. +49 211 97 177 477 · www.iloq.de
Making life accessible: iLOQ ermöglicht Menschen, Unternehmen und Organisationen die Unabhängigkeit von mechanischen Schließzylindern und Schlüsseln.

Zeit + Zutritt

primion Technology GmbH
Steinbeisstraße 2-4 · 72510 Stetten a.K.M.
Tel.: 07573/952-0 · Fax: 07573/92034
info@primion.de · www.primion.de
Arbeitszeitmanagement, Zugangsmanagement, Personaleinsatzplanung, grafisches Alarmmanagement, SAP-Kommunikationslösungen, Ausweiserstellung, Biometrie

Notruf- und Service-Leitstelle

HWS Wachdienst Hobeling GmbH
Am Sportpark 75 · D-58097 Hagen
Tel.: (0 23 31) 47 30 -0 · Fax: -130
hobeling@hobeling.com · www.hws-wachdienst.de
VdS-Notruf- und Service-Leitstelle, Alarmempfangsstelle DIN EN 50518, Alarmprovider, Mobile Einsatz- und Interventionskräfte, Objekt- und Werkschutz

Zeit + Zutritt

IntraKey technologies AG
Wiener Str. 114-116 · 01219 Dresden
Tel.: 0351/31558-0 · Fax: 0351/31558-129
info@intrakey.de · www.intrakey.de
Zutrittskontrolle, Zeiterfassung, Raumvergabe, Elektronische Schließfächer, Fuhrparkmanagement, Bezahlen, BikeParkBox

Notruf- und Service-Leitstelle

FSO Fernwirk-Sicherheitssysteme Oldenburg GmbH
Am Patentbusch 6a · 26125 Oldenburg
Tel.: 0441-69066 · info@fso.de · www.fso.de
Alarmempfangsstelle nach DIN EN 50518
Alarmprovider und Notruf- und Service Leitstelle nach VdS 3138, zertifiziertes Unternehmen für die Störungsannahme in der Energieversorgung.

Zeit + Zutritt

Morphean SA – Headquarter
Route du Jura 37
1700 Fribourg · Switzerland
Tel. +41 26 422 00 90
info@morphean.ch · www.morphean.com
Video Surveillance as a Service (VSaaS) und Access Control as a Service (ACaaS) – Videoüberwachung und Zugangskontrolle mit KI und Cloud.

Zeit + Zutritt

SALTO Systems GmbH
Schwelmer Str. 245 · 42389 Wuppertal
Tel.: +49 202 769579-0 · Fax: +49 202 769579-99
info.de@saltosystems.com · www.saltosystems.de
Vielseitige und maßgeschneiderte Zutrittslösungen - online, offline, funkvernetzt, Cloud-basiert und mobil.

BRAND SCHUTZ

Zeit + Zutritt

Paxton Access GmbH
Westhoffstr. 128
D–48159 Münster
Phone: +49 (0)251 2080 6900
E-mail: verkauf@paxton-gmbh.de
Internet: www.paxton-access.com/de

Paxton nutzt die neueste Technologie, um leistungsstarke und dennoch einfach zu installierende und zu verwendende Sicherheitslösungen anzubieten. Das Produktportfolio umfasst vernetzte Zugangskontrolllösungen, kabelgebundene und kabellose Steuerungen, Video-Türsprechanlage und Videoüberwachung.

Zeit + Zutritt

sesamsec GmbH
Finsterbachstraße 1 · 86504 Merching, Germany
Tel.: +49 8233 79445-0 · Fax: +49 8233 79445-20
info@sesamsec.com · www.sesamsec.com
Anbieter von Zutrittskontrollsystemen, von Einzeltürlösungen bis zu intelligenten Campus-Systemen. Hardware und innovative Softwarelösungen wie Physical Access Control-as-a-Service (PACaaS).

Brandschutz

DENIOS SE
Dehmer Straße 54-66
32549 Bad Oeynhausen
Fachberatung: 0800 753-000-3
Gefahrstofflagerung, Brandschutzlager, Brandschutz für Lithium-Akkus, Wärme- und Kältekammern, Containment, Auffangwannen, Arbeitsschutz, sicherheitsrelevante Betriebsausstattung, Gefahrstoff-Leckage-Warnsystem

Zeit + Zutritt

PCS Systemtechnik GmbH
Pfälzer-Wald-Straße 36 · 81539 München
Tel.: 089/68004-0 · Fax: 089/68004-555
intus@pcs.com · www.pcs.com
Zeiterfassung, Gebäudesicherheit, Zutritts- und Zufahrtskontrolle, Biometrie, Video, Besuchermanagement, SAP, Handvenenerkennung

Zeit + Zutritt

TIL TECHNOLOGIES GMBH
Haus 3 · Eisenstraße 2-4
D-65428 Rüsselsheim
Tel. 06142/481 00-66
vertrieb@til-technologies.de
www.til-technologies.de
Zertifizierte Zutrittskontrolle, Gebäudemanagement, Besuchermanagement, Sicherheitstechnik, RFID-Lesegeräte, cybersichere Zutrittskontrolle, BSI-konforme Zutrittskontrolle, Zutrittskontrolle für KRITIS .

Brandschutz

Hertek GmbH
Landsberger Straße 240
12623 Berlin
Tel.: +49 (0)30 93 66 88 950
info@hertek.de · www.hertek.de
Hertek: ein Unternehmen im Bereich Brandschutzlösungen. Branchenspezifisches Fachwissen mit hochwertigen Brandschutzkomponenten vereint zu einem sicheren und verlässlichen Brandschutz. Flankiert wird dies mit Fachschulungen und einen umfangreichen, lösungsorientierten Kundenservice.

Brandschutz

Labor Strauss Gruppe
Firmensitz: Wiegelestraße 36 · A-1230 Wien
Tel.: +43 1 521 14-0
office@lst.at · www.laborstrauss.com
Standorte: Wien, Graz, Innsbruck, Pockau-Lengefeld, Mönchengladbach, Hamburg, Augsburg
Die Spezialisten für Brandmeldeanlagen, Löschsteuersysteme und Notbeleuchtung

ARBEITS SICHERHEIT

Maschinen + Anlagen

K.A. Schmersal GmbH & Co. KG
Möddinghofe 30 · 42279 Wuppertal
Tel.: 0202/6474-0 · Fax: 0202/6474-100
info@schmersal.com · www.schmersal.com
Sicherheitszuhaltungen und Sicherheitssensoren, optoelektronische Sicherheitseinrichtungen wie Sicherheitslichtschranken sowie Sicherheitsrelaisbausteine, programmierbare Sicherheitssteuerungen und die Safety Services des Geschäftsbereichs tec.nicum

Brandschutz

Prymos GmbH
Siemensstraße 18 · 63225 Langen
Tel.: 06103/4409430 · Fax: 06103/4409439
info@prymos.com · www.prymos.com
ASR A2.2 kompatible Feuerlöscher-Sprays.
Bis zu 10 Jahre wartungsfreie DIN EN 3 Feuerlöscher.

Arbeitssicherheit

ELTEN GmbH
Ostwall 7–13 · 47589 Uedem
Tel.: 02825/8068
www.elten.com · service@elten.com
Sicherheitsschuhe, Berufsschuhe, PSA, ELTEN, Berufsbekleidung, Sicherheit

Maschinen + Anlagen

Leuze electronic GmbH & Co. KG
In der Braike 1 · D-73277 Owen
Tel.: +49(0)7021/573-0 · Fax: +49(0)7021/573-199
info@leuze.com · www.leuze.com
Optoelektronische Sensoren, Identifikations- und Datenübertragungssysteme, Distanzmessung, Sicherheits-Sensoren, Sicherheits-Systeme, Sicherheits-Dienstleistungen

Brandschutz

Securitas Electronic Security Deutschland GmbH
SeTec Sicherheitstechnik
Haupstr. 40 a · 82229 Seefeld
Tel.: +49(0)8152/9913-0 · Fax: +49(0)8152/9913-20
info@setec-security.de · www.setec-security.de
Handfeuermelder, Lineare Wärmemelder, Feuerwehr Schlüsseldepots, Feuerwehr, Schlüsselmanager, Feuerwehrperipherie, Feststellanlagen, Störmeldezentralen

Arbeitssicherheit

Hailo-Werk
Rudolf Loh GmbH & Co. KG
Daimlerstraße 8 · 35708 Haiger
www.hailo-professional.de
professional@hailo.de
Steig-/Schachtleitern, Steigschutzsysteme, Schachtabdeckungen, Servicelifte, Schulungsangebote

Maschinen + Anlagen

Pepperl+Fuchs SE
Lilienthalstraße 200 · 68307 Mannheim
Tel.: 0621/776-1111 · Fax: 0621/776-27-1111
fa-info@de.pepperl-fuchs.com
www.pepperl-fuchs.com
Sicherheits-Sensoren, Induktive-, Kapazitive-, Optoelektronische und Ultraschall-Sensoren, Vision-Sensoren, Ident-Systeme, Interface-Bausteine

Brandschutz

WAGNER Group GmbH
Schleswigstraße 1–5 · 30853 Langenhagen
Tel.: +49 (0)511 97383 0
info@wagnergroup.com · www.wagnergroup.com
Brandfrüherkennung und Brandmeldeanlagen, Brandvermeidung, Brandbekämpfung, Gefahrenmanagement

Arbeitssicherheit

HAIX Schuhe Produktions- und Vertriebs GmbH
Auhofstraße 10 · 84048 Mainburg
Tel.: 08751/8625-0 · Fax: 08751/8625-25
info@haix.de · www.haix.com
Hochwertige Funktionsschuhe für Feuerwehr und Rettungsdienst, Polizei und Militär, Bau und Handwerk, Forstwirtschaft, Jagd und Freizeit. Berufs- und Funktionskleidung. Made in Europe.

Maschinen + Anlagen

Pizzato Deutschland GmbH
Brienner Straße 55 · 80333 München
Tel.: 01522/5634596 · 0173/2936227
aspg@pizzato.com · www.pizzato.com
Automatisierung, Maschinen- und Anlagensicherheit: Sensorik, Schalter, Zuhaltungen, Module, Steuerungen, Mensch-Maschine-Schnittstelle, Positions- und Mikroschalter, Komponenten für die Aufzugsindustrie, u.v.m.

GASMESS TECHNIK

MASCHINEN ANLAGEN SICHERHEIT

Maschinen + Anlagen

R3 Solutions GmbH
Kurfürstendamm 21 · 10719 Berlin · Deutschland
Tel.: +49 30 800 936 75
contact@r3.group · www.r3.group
Entwicklung und Vertrieb industriefähiger Funktechnologie. Kernprodukt ist die EchoRing-basierte Bridge E: eine Plug-and-Play-Netzwerklösung für ausfallsichere Kommunikation mit geringer Latenz. Kernanwendungsgebiete finden sich in der Automatisierung sowie im Transport- und Logistik-Bereich.

Gasmesstechnik

GfG Gesellschaft für Gerätebau mbH
Klönnestraße 99 · D-44143 Dortmund
Tel.: +49 (0)231/56400-0 · Fax: +49 (0)231/56400-895
info@gfg-mbh.com · GfGsafety.com
Gaswarntechnik, Sensoren, tragbare und stationäre Gasmesstechnik

Maschinen + Anlagen

EUCHNER GmbH + Co. KG
Kohlhammerstraße 16
D-70771 Leinfelden-Echterdingen
Tel.: 0711/7597-0 · Fax: 0711/753316
www.euchner.de · info@euchner.de
Automation, MenschMaschine, Sicherheit

Maschinen + Anlagen

SSP Safety System Products GmbH & Co. KG
Max-Planck-Straße 21 · DE-78549 Spaichingen
Tel.: +49 7424 980 490 · Fax: +49 7424 98049 99
info@ssp.de.com · www.safety-products.de
Dienstleistungen & Produkte rund um die Maschinensicherheit: Risikobeurteilung, Sicherheitssensoren, -Lichtvorhänge, - Zuhaltungen, -Steuerungen sowie Schutzumhausungen, Zustimmtaster uvm.

GEFAHRSTOFF MANAGEMENT

Gefahrstoffmanagement

DENIOS SE
Dehmer Straße 54-66
32549 Bad Oeynhausen
Fachberatung: 0800 753-000-3
Gefahrstofflagerung, Brandschutzlager, Brandschutz für Lithium-Akkus, Wärme- und Kältekammern, Containment, Auffangwannen, Arbeitsschutz, sicherheitsrelevante Betriebsausstattung, Gefahrstoff-Leckage-Warnsystem

UNTERBRECHUNGSFREIE STROMVERSORGUNG

Gefahrstoffmanagement

asecos GmbH
Sicherheit und Umweltschutz
Weiherfeldsiedlung 16–18 · 63584 Gründau
Tel.: +49 6051 9220-0 · Fax: +49 6051 9220-10
info@asecos.com · www.asecos.com
Gefahrstofflagerung, Umwelt- unad Arbeitsschutz, Sicherheitsschränke, Chemikalien- und Umluftschränke, Druckgasflaschenschränke, Gefahrstoffarbeitsplätze, Absauganlagen, Raumluftreiniger uvm.

Gefahrstoffmanagement

SÄBU Morsbach GmbH
Zum Systembau 1 · 51597 Morsbach
Tel.: 02294 694-23 · Fax: 02294 694-38
safe@saebu.de · www.saebu.de
Gefahrstofflagerung, Gefahrstoffcontainer, Arbeits- & Umweltschutz, Auffangwannen, Fassregale, Regalcontainer, Brandschutzschränke, Gasflaschenlagerung, Gasflaschenbox

Unterbrechungsfreie Stromversorgung

NSGate
2F, No.53-16, Shcherbakovskaya Straße
105187 Moskau, Russland
Tel.: +7 495 139 6903
www.nsgate.eu · sales@nsgate.com
DC-USVs 150-500VA, off-grid solar systems und hochwertige Produkte für Videoüberwachungssysteme im Außenbereich. Mikroklima-Komponenten für Außengehäuse: Heizgerät, Kühlen, Thermostate. Industrielle PoE-Switches, Ethernet-Extenders und Überspannungsschutzgeräte.

Gefahrstoffmanagement

BAUER GmbH
Eichendorffstraße 62 · 46354 Südlohn
Tel.: + 49 (0)2862 709-0 · Fax: + 49 (0)2862 709-156
info@bauer-suedlohn.com · www.bauer-suedlohn.com
Auffangwannen, Brandschutz-Container, Fassregale, Gefahrstofflagerung, Regalcontainer, Wärmekammern, individuelle Konstruktionen

Ihr Eintrag in der Rubrik

GIT BusinessPartner
Die Einkaufsrubrik für den direkten Kontakt

Schicken Sie einfach eine E-Mail an miryam.reubold@wiley.com

Wir beraten Sie gerne!

DAS VIP INTERVIEW

Dr. Swantje Westpfahl

Direktorin, Geschäftsführerin und Strategische Leitung des Institute for Security and Safety GmbH

- Gremien-Mitglied der OEWG der Vereinten Nationen für IKT im Kontext der internationalen Sicherheit und in der WP.29 GRVA der UNECE
- Leiterin der Task Force European Initiatives des EE-ISAC
- Mitwirkende in zwei Arbeitsgruppen beim World Economic Forum
- Promotion im Bereich Computerlinguistik an der Universität Mannheim

Die volle Version des Interviews finden Sie hier:

Menschen machen Märkte
In jeder Ausgabe Ihrer GIT SICHERHEIT bitten wir wichtige Personen, Entscheider, Menschen aus der Sicherheitsbranche, zum VIP-Interview.

Ihr Berufswunsch mit 20 war:
Diplomatin. Die Idee, Menschen auf internationaler Ebene dazu zu bringen, in schwierigen Fällen miteinander zu kommunizieren und gemeinsam eine friedliche und gute Lösung für alle Beteiligten zu finden – das fasziniert mich bis heute.

Was hat Sie dazu bewogen, eine Aufgabe im Bereich Sicherheit zu übernehmen?
Durch meine Promotion im Bereich Computerlinguistik hatte ich erste Berührungspunkte mit Datensicherheit. Auch privat habe ich mir sehr viele Gedanken zu diesem Thema gemacht. Da ich von Natur aus immer bestrebt bin, mehr und Neues zu lernen, schien es mir naheliegend, mich in der Wirtschaft in den Bereich der (Cyber-)Sicherheit zu begeben – gerade weil man dort die Möglichkeit hat, durch Kommunikation viel Positives für einzelne Unternehmen aber auch unsere Gesellschaft zu bewirken.

Welche sicherheitspolitische Entscheidung oder welches Projekt sollte Ihrer Meinung nach schon längst umgesetzt sein?
Auf internationaler Ebene die finanzielle und strukturelle Stärkung der ISACs (Information Sharing and Analysis Centers). Sie haben das Potenzial, Interessengruppen- und Sektorenspezifisch für einen vertrauensvollen Austausch von Bedrohungen und Best Practices zu sorgen, sind aber bisher nahezu vollständig auf ehrenamtliche Arbeit angewiesen.
Auf ganz anderer Ebene würde ich mir stärkere Kontrollen für die Cybersicherheit von Produkten für Endverbraucher wünschen – insbesondere für IoT-Geräte.
Als Drittes wünsche ich mir eine viel bessere Aufstellung der Polizei und der Bundeswehr in Sachen Cyber-Defense, Incident Response und Forensik. Ich sehe, dass es langsam ein Umdenken gibt, jedoch ist an der Stelle noch viel zu wenig Personal vorhanden.

Wer hat Ihrer Meinung nach eine Auszeichnung verdient?
Mein gesamtes Team. Jede und jeder einzelne von ihnen hat einen vollkommen unterschiedlichen beruflichen Hintergrund und ebenfalls sehr unterschiedliche Wesensarten. Ich bewundere den gegenseitigen Respekt, die Unterstützung und den Humor, mit dem Projekte angepackt werden. Wir sind nach dem plötzlichen Tod unseres Geschäftsführers durch eine sehr schwierige Phase gegangen und für den Zusammenhalt und die Anstrengungen in der Transition hat mein Team ehrlich eine Auszeichnung verdient!

Wie würde ein guter Freund Sie charakterisieren? Ich habe einem Freund diese Frage weitergeleitet: Unerschütterlich optimistisch, verliert nie die gute Laune. Sie hat ein aufgeschlossenes, hilfsbereites und freundliches Wesen, wodurch sie schnell Kontakte knüpft. Sie kann schnell neue Zusammenhänge verstehen, ist offen für neue Ideen und diskussionsfreudig. Sie ist die Art von Person, die einen auch an einem Montagmorgen davon überzeugen kann, dass es einen Freitagabend geben wird. So begeistert und motiviert sie andere.

Welches Buch haben Sie zuletzt gelesen?
Ich lese generell nahezu alles, was man mir in die Hand drückt: von Theodor Storm bis Science Fiction. Zuletzt habe ich „Eine Frage der Chemie“ gelesen. Das Buch hat mich fasziniert und mich ins Grübeln gebracht. Ich bin dankbar, dass ich weder in der Wissenschaft noch in meiner jetzigen Karriere je größere Probleme aufgrund meines Geschlechts erleben musste. Ich denke auch, dass viele von uns nachhaltig von der #metoo-Debatte profitieren, wenn man das überhaupt so ausdrücken kann. Richtig ist aber auch, dass ich häufig viel zu wenig andere Frauen auf Fachkonferenzen treffe (beispielsweise war ich neulich eine von 4 Frauen bei 116 Teilnehmenden einer Fachkonferenz).

Was motiviert Sie?
Wenn ich sehe, wie Menschen um mich herum über sich selbst hinauswachsen und dass unsere Arbeit einen Impact hat.

Worüber machen Sie sich Sorgen?
Wir leben in einer Zeit, in der unsere Gesellschaft unweigerlich mit der Digitalisierung der Lebenswelt verbunden ist. Darüber hinaus sind Bedrohungen für jeden Einzelnen nicht mehr geografisch zu erfassen und Gefahren im Internet für viele nicht so leicht erkennbar. Viele Apps und Geräte müssen den Nutzer vor allem in Bezug auf ihre Funktionalität überzeugen. Das birgt ein Risiko, da es eine gewisse Vorbildung im Bereich sicheres Verhalten im digitalen Raum voraussetzt. Diese nehme ich in unserer Gesellschaft nicht ausreichend wahr. Die Basis für den technologischen Fortschritt sollte immer begleitet werden von den Security-by-Design-Prinzipien – in der Realität wird meist zunächst entwickelt und dann die Cybersicherheit irgendwie nachgezogen, wenn überhaupt.

Die beste Erfindung im Bereich Sicherheit ist Ihrer Meinung nach:
Es ist sehr schwierig, etwas als DIE beste Erfindung zu definieren, und die nächste Frage wäre, für welche Sicherheit? Im Bereich der Informationssicherheit ist die wohl älteste und beste Erfindung immer noch die Verschlüsselung. Tolle Technologien, die Digitalisierung für Endanwender sicherer machen, sind allerdings auch Firewalls, Public Key Infrastructure, VPNs, Multifaktor-Authentifizierung sowie Standards für Managementsysteme.

SICHERHEITS EXPO München

28.–29. Juni 2023

Die Fachmesse für

Zutrittskontrolle
Videoüberwachung
Brandschutz
Perimeter Protection
IT-Security

www.sicherheitsexpo.de


CONNEXIS
SAFETY+
GORE-TEX
HAIX®
Dein Plus an
SICHERHEIT,
Komfort und LEISTUNG!
HEROES
WEAR
HAIX